YEAR 2000 COMPUTER PROBLEM: DID THE WORLD OVERREACT, AND WHAT DID WE LEARN?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

AND THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JANUARY 27, 2000

Committee on Government Reform

Serial No. 106–149

Committee on Science

Serial No. 106–84

Printed for the use of the Committee on Government Reform and the Committee on Science

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

66–711 CC WASHINGTON : 2000

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
LISA SMITH ARAFUNE, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
BONNIE HEALD, *Director of Communications/Professional Staff Member*
CHIP AHLSWEDE, *Clerk*
MICHELLE ASH, *Minority Counsel*
TREY HENDERSON, *Minority Counsel*

COMMITTEE ON SCIENCE

F. JAMES SENSENBRENNER, JR., (R-Wisconsin), *Chairman*

SHERWOOD L. BOEHLERT, New York
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan*
DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California
JUDY BIGGERT, Illinois
MARSHALL "MARK" SANFORD, South Carolina
JACK METCALF, Washington
RALPH M. HALL, Texas, RMM**
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
BRIAN BAIRD, Washington
JOSEPH M. HOEFFEL, Pennsylvania
DENNIS MOORE, Kansas
JOE BACA, California

CONTENTS

YEAR 2000 COMPUTER PROBLEM: DID THE WORLD OVERREACT, AND WHAT DID WE LEARN?

THURSDAY, JANUARY 27, 2000

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY, COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON TECHNOLOGY, COMMITTEE ON SCIENCE,

Washington, DC.

The subcommittees met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the Subcommittee on Government Management, Information, and Technology) presiding.

Present for the Subcommittee on Government Management, Information, and Technology: Representatives Horn, Biggert, Walden, and Turner.

Staff present for the Subcommittee on Government Management, Information, and Technology: J. Russell George, staff director and chief counsel; Mathew Ryan, senior policy director; Bonnie Heald, director of communications and professional staff member; Chip Ahlswede, clerk; Deborah Oppenheim, intern; Michelle Ash and Trey Henderson, minority counsels; and Jean Gosa, minority clerk.

Present for the Subcommittee on Technology: Representatives Morella, Green, Barcia, Wu, and Baird.

Staff present for the Subcommittee on Technology: Jeff Grove, staff director; Ben Wu, counsel; Michael Quear, minority professional staff member; and Marty Ralston, minority staff assistant.

Mr. HORN. This joint hearing of the House Subcommittee on Government Management, Information, and Technology, and the House Subcommittee on Technology will come to order.

It is now 27 days into the new millennium. The lights are still on, telephones keep ringing, and the airplanes are still flying. So far, the biggest challenge, at least here on the east coast, is shoveling through the mountainous snowdrifts dumped by the first major storm of the year 2000. Thanks to the hard work of thousands of dedicated people at a cost in the billions of dollars, we have the luxury of meeting today to discuss the benefits that have been derived from the year 2000 computer challenge.

Over the past 4 years, these subcommittees have spent countless hours examining the Federal Government's computer preparations for the year 2000, or Y2K. When we began this process in April 1996, two Cabinet Secretaries had never heard of Y2K, much less

begun preparing for it. That ultimately changed, but not without congressional prodding through 43 hearings and 10 report cards, grading agencies on their progress. In addition to fixing all of the government's 6,400 mission-critical computer systems, the subcommittees expected agencies to develop viable contingency plans in case those computer fixes did not work. We prodded, we questioned, and we hoped for the best, and the best happened. The Federal Government experienced a successful transition into the new millennium.

Some glitches did occur, however, giving cause to wonder what might have happened if the work had not been completed. I am inserting in the hearing record a statement stressing that without the work of many in the executive and legislative branches, it would not have been as successful.

Without objection, that will be in the record at this point.

The Defense Department had problems with its surveillance satellites. Some retailers were unable to process customer credit card purchases. A Chicago area bank was unable to process Medicare payments. As far as we know, those isolated problems were quickly repaired. Some still question whether other incidents might have occurred, but were unexpected due to a fix first, report later mentality.

Successfully meeting the year 2000 challenge has provided many lessons that must not be ignored or forgotten. The unextendable deadline forced government leaders to focus on information technology issues. Program and technology personnel worked intensely and closely to get the job done. In addition, government agencies and private sector organizations were forced to develop detailed inventories of their technology resources and computer systems, in many cases for the first time. Unnecessary and obsolete systems have hopefully been discarded.

Finally, government agencies and their partners have tested and retested data flows at unprecedented levels. Strong teamwork and rugged determination solved the year 2000 problem.

Some critics now question whether the high cost of this massive effort was necessary. The best estimates currently indicate that the executive branch will spend more than $8 billion on year 2000 fixes. The Secretary of Commerce has reported that the United States will have spent about $100 billion on the effort as a whole.

Was that money well spent? Of course it was.

The executive branch of the Federal Government has not always been known as a careful steward of the citizens' money, regardless of what party is in power. Large corporations have waste also, and those that are publicly traded could not afford to squander hundreds of millions of dollars on unnecessary computer problems and contingency plans. Boards of directors and stockholders would not permit it. Whether large or small, successful businesses rarely fritter away money. This was a massive problem that required a massive solution.

We are grateful to everyone who contributed the many ideas, solutions, and hard work that led to the success of this effort, from government personnel to grassroots organizations and the private sector. Thank you all for a job well done.

Today we welcome some of those dedicated leaders. The Honorable John Koskinen, Assistant to the President and Chair of the President's Council on Year 2000 Conversion; Mr. Joel Willemssen, Director of Civil Agencies Information Systems for the General Accounting Office; the Honorable Charles Rossotti, Commissioner of Internal Revenue; Mr. Fernando Burbano, Chief Information Officer of the Department of State and cochairman of the Security Privacy and Infrastructure Committee of the Chief Information Officer Council; Mr. Harris Miller, president of Information Technology Association of America; Ms. Kathy Hotka, vice president for Information Technology of the National Retail Federation; and, last, Mr. Gary Beach, publisher of the CIO Communications, Inc. I might say that is a very distinguished magazine, and I read it regularly. We welcome each of you, and look forward to your testimony.

It is a pleasure to first introduce Mr. John Koskinen, special assistant to the President, Chairman, President's Council on Year 2000 Conversion.

[The prepared statement of Hon. Stephen Horn follows:]

House Subcommittee on Government Management, Information, and Technology

---

Opening Statement
Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
January 27, 2000

This joint hearing of the House Subcommittee on Government Management, Information, and Technology, and the House Subcommittee on Technology will come to order.

It is now 27 days into new millennium. The lights are still on; telephones keep ringing; and the airplanes are still flying. So far, the biggest challenge, at least here on the East Coast, is shoveling through the mountainous snowdrifts dumped by the first major storm of the year 2000. Thanks to the hard work of thousands of dedicated people at a cost in the billions of dollars, we have the luxury of meeting today to discuss the benefits that have been derived from the Year 2000 computer challenge.

Over the past four years, these subcommittees have spent countless hours examining the Federal Government's computer preparations for the Year 2000 or Y2K. When we began this process in April 1996, two cabinet secretaries had never heard of Y2K, much less begun preparing for it. That ultimately changed, but not without congressional prodding through 43 hearings and 10 report cards, grading agencies on their progress. In addition to fixing all of the Government's 6,400 mission-critical computer systems, the subcommittees expected agencies to develop viable contingency plans, in case those computer fixes did not work. We prodded. We questioned. We hoped for the best. And the best happened. The Federal Government experienced a successful transition into the new millennium.

Some glitches did occur, however, giving cause to wonder what might have happened if the work had not been completed. I am inserting in the hearing record a statement, stressing that without the work of many in the executive and legislative branches, it would not have been as successful.

The Defense Department had problems with its surveillance satellites. Some retailers were unable to process customer credit card purchases. A Chicago-area bank was unable to process Medicare payments. As far as we know, these isolated problems were quickly repaired. Some still question whether other incidents might have occurred, but were unreported due to a "fix first, report later" mentality.

Successfully meeting the Year 2000 challenge has provided many lessons that must not be ignored or forgotten. The unextendable deadline forced government leaders to focus on information technology issues. Program and technology personnel worked intensely and closely to get the job done. In addition, government agencies and private sector organizations were forced to develop detailed inventories of their technology resources and computer systems – in many cases, for the first time. Unnecessary and obsolete systems have hopefully been discarded. Finally, government agencies and their partners have tested and re-tested data flows at unprecedented levels. Strong teamwork and rugged determination solved the Year 2000 problem.

Some critics now question whether the high cost of this massive effort was necessary. The best estimates currently indicate that the executive branch will spend more than $8 billion on its Year 2000 fixes. The Secretary of Commerce has reported that the United States will have spent about $100 billion on the effort.

Was that money well spent? Of course, it was.

The executive branch of the Federal Government has not always been known as a careful steward of its citizens' money. Large corporations have waste also, but those that are publicly traded could not afford to squander hundreds of millions of dollars on unnecessary computer problems and contingency plans. Boards of Directors and stockholders would not permit it. Whether large or small, successful businesses rarely fritter away money. This was a massive problem that required a massive solution.

We are grateful to everyone who contributed the many ideas, solutions, and hard work that led to the success of this effort – from government personnel to grassroots organizations and the private sector. Thank you for a job well done. Today, we welcome some of those dedicated leaders.

- The Honorable John Koskinen, Assistant to the President and Chair of the President's Council on Year 2000 Conversion;
- Mr. Joel Willemssen, Director of Civil Agencies Information Systems for the General Accounting Office;
- The Honorable Charles Rossotti, Commissioner of Internal Revenue;
- Mr. Fernando Burbano, Chief Information Officer of the Department of State and co-chairman of Security Privacy and Critical Infrastructure for the CIO Council;
- Mr. Harris Miller, President of Information Technology Association of America;
- Ms. Cathy Hotka, Vice President for Information Technology of the National Retail Federation; and
- Mr. Gary Beach, Publisher, CIO Communications, Inc.

We welcome each of you, and look forward to your testimony.

Mr. HORN. I now yield for opening statement from the cochairman of the task force, Mrs. Morella, the gentlewoman from Maryland.

Mrs. MORELLA. Thank you very much, Mr. Chairman. We will hear from Mr. Koskinen and the very prominent panel very shortly.

I appreciate having this hearing. I think it is important that we look back at what has happened, and in particular, look ahead to the future. If I had told everyone in this room a month ago that in January 2000 the Federal Government would shut down for 2 days and virtually the entire southeast and northeast would be crippled, most likely everyone would have immediately blamed Y2K millennium bug and not mother nature. Yet it took a blizzard of snow and ice to accomplish what many doomsayers had predicted long ago for the millennium bug. So how is it that a winter storm caused more damage and inconveniences than the Y2K problem?

In the ensuing weeks since the passage of January 1, 2000, similar questions have been posted. Was the Y2K problem real or was it overhyped? Was the $100 billion spent in the United States, roughly $365 for every American citizen overall? Did all of our efforts stave off an impending disaster, or was Y2K simply a nonevent waiting to happen?

In my mind, there is no doubt the problem was real. From the very first hearing that my technology subcommittee conducted in the spring of 1996, to right up to the final month of December 1999, we witnessed systems failing Y2K tests and crashing completely. Our concern for the Y2K issue was initially so great and disturbing that we have held almost 100 hearings in both the House and the Senate on the issue, which I understand makes Y2K the single most thoroughly investigated issue ever in the history of congressional oversight.

Ultimately, I believe two factors tipped the balance from the grave uncertainty many of us harbored in the beginning. The first was that we all knew the Y2K problem would strike on a certain date, January 1, 2000, thereby allowing us to collectively plan, coordinate and collaborate toward that deadline.

The other and more significant factor was that after over a year and a half of persistent cajoling by Congress, after we realized this, our Nation required executive action to effectively combat the Y2K problem, the President finally exercised his authority in the spring of 1998. Y2K was suddenly catapulted to become a top administration management priority, and John Koskinen was appointed to oversee our Federal Government's efforts and to partner with our Nation's private sector and with other countries internationally.

John certainly deserves a great deal of accolades for his stewardship. The well-deserved cheers I wanted to point out to for our victory in vanquishing the millennium bug should also go to those who ably served in the front lines of this epic battle, all the dedicated Federal employees, public servants and professionals who were the technicians, and those who gave countless hours on their holidays to provide assurance to the American people that our Nation would be prepared for Y2K.

I think the fact that nothing of disastrous proportions happened does not mean that nothing would have happened. For example,

the American Banking Association reported that, but for the $10 billion in Y2K fixes, mortgage calculations would have been incorrect, direct deposit of pay and government benefits would have been problematic, and credit cards could not be read due to problems with expiration dates.

Similarly, the telecommunications industry reported that the $3.6 billion that they spent over the past 3 to 4 years prevented the potential gradual deterioration of public switch telephone network performance, including slow response times for dial tone access as well as interruptions of service.

The result of our Y2K experience is a testament to the fact that we prepared well and we invested properly.

I believe, however, the investments were not just about Y2K, but also about improving our Nation's information technology systems and gaining knowledge about those systems. That is the focus of our hearing today. This hearing is not designed to simply pat each other on the back or to allow our panelists to take a figurative victory lap around the witness table, but to ascertain the lessons that we learned from our Y2K experience.

Will Y2K inspire a conscious effort for greater long-term planning and more reliable and secure technology, or will it just prolong the shortsighted thinking that made Y2K so costly?

While many systems have relays replaced, some programs were fixed by applying a Y2K patch that will require another round of fixes within the next two decades. I look forward to addressing these and many other issues with our distinguished panel of witnesses, most of whom have appeared before us on many occasions. It is only appropriate that since this is the absolutely positively final last and ultimate hearing of the House Y2K Task Force, we close with those who have been involved with this issue since the very beginning.

Perhaps this hearing can provide the foundation for initiatives as we address the 5-digit computer date problem, Y10K as it may come to be known. If so at that time, maybe Steve Horn and I can chair that task force, along with Strom Thurmond in the Senate.

I would like to extend my deep appreciation to all the members of my technology subcommittee and Congressman Horn's government management subcommittee and his leadership for the 4 years of vigilant and cooperative bipartisan initiatives, and I especially want to acknowledge the hard work of my ranking member, Jim Barcia, and certainly Chairman Horn, the distinguished cochair of the task force, and Jim Turner of the government management subcommittee, ranking member, and the members of both subcommittees who have been very dedicated, and I yield back. Thank you.

Mr. HORN. We thank you so much for your nice words for all the Members, and all of our witnesses. We agree with you, and I am delighted to now yield to the gentleman who has been here right from the beginning of his duties as the ranking member on the side of the subcommittee on government management, Mr. Turner from Texas. We are delighted you could make it out of the snow, if you have any down there, and into Washington for this meeting. So thank you very much for all you have done to help us in the field hearings and everywhere else.

Mr. TURNER. Thank you, Mr. Chairman. When I left Texas the other day, it was 80 degrees.

I want to commend you, Mr. Chairman, and Chairwoman Morella, for the good work you have done. This task force and these two committees were about a 3½-year project. As I recall, my staff advised me we had 24 different hearings of this subcommittee alone on this subject. Many observers say that the Y2K problem was the greatest management challenge the Federal Government has faced, and perhaps that is true. I think most of us had a high degree of confidence after the many hearings that we had that we would make it through January 1st without great problems, but nobody really knew for sure. The fact we did make it I am sure is due, in large part, to the hard work you, Mr. Chairman, and Chairwoman Morella, have made in an effort to make sure the Federal Government is ready.

I also want to commend the ranking member of the science subcommittee, Mr. Barcia, and I want to thank Mr. Williamson. He worked very diligently, met with this committee time and time again, and I think, in large part, usual efforts helped us get to where we needed to go.

Of course, Mr. Koskinen and the President's Y2K council, I think, did an outstanding job. I really felt sorry for you when I was watching you on television on New Year's Day and you kept holding these press conferences with nothing to say. That is the worst nightmare of any politician, that somehow we would have a press conference and there is nothing to say. But you seemed to have survived it well, and you and your council did an outstanding job working not only with the public sector and Federal agencies, but reaching out to the private sector to ensure that we got to where we needed to go.

That is not to say there weren't significant potential problems. As I recall from many of our hearings, we tried to ask witnesses that came before us to tell us what they fixed, what would happen if they had not been diligent about remediation of their Y2K problems, and some of the stories we heard clearly convinced me that all of the effort and all of the work that took place was needed, did accomplish the desired result, and the fact that we had no great crisis on January 1 was to the credit of all of those many thousands of people who spent countless hours and millions of dollars to remediate the problem.

We are here today not to congratulate ourselves, but to look back and to review the results of our efforts, to see what lessons we have learned. I feel confident we are better prepared as a Nation to meet a future national emergency than we have ever been in terms of keeping our computer systems working, which, of course, every facet of our life now depends upon our computers working well.

So I think we are going to have a good hearing today, and I appreciate all the witnesses being here. Again, I would like to thank Chairman Horn and Chairwoman Morella for the good work that you did.

Mr. HORN. Well, thank you very much. You have sure been with us since the ground floor, and we have another person who has been with us ever since she has been elected to Congress, and the gentlewoman from Illinois, Mrs. Biggert, we have held hearings in

her area, which is a wonderful suburb outside of Chicago, and we appreciate your regular attendance at these meetings and the contributions you have made in staff meetings and Member meetings. So thank you very much for coming to this hearing. The gentlewoman from Illinois, Mrs. Biggert.

Mrs. BIGGERT. Thank you, Chairman Horn and Chairwoman Morella. Let me thank you for calling this hearing on the impact of the Y2K date change. Contrary to what some people felt might happen, the planes didn't fall from the sky when the clock struck midnight, telephones retained their dial tones, water still ran from the faucets and America's New Year's celebrations were not left in the dark. So I think we had a good new year.

But remarkably, and a little bit surprisingly, substantial Y2K problems were not experienced out of this country either, despite the lack of preparation on the part of some of the nations' computers and other essential services across the globe. We really saw no major disruptions.

But as this committee heard numerous times during its hearings, Y2K-related glitches could have had a substantial and extremely negative impact on the variety of services, the smooth turnover from 1999 into 2000 is directly related, I think, to the billions of dollars and hundreds of man-hours directed toward preventing and correcting potential Y2K problems. I think it goes without saying that from what we have seen, or seen thus far relating to Y2K disruptions, that these efforts paid off handsomely. Y2K preparations paid off in other ways as well as a result of the Y2K concerns; there are now thousands more American families that own the equipment, such as generators needed to prepare for other types of emergencies, namely snowstorms, floods and hurricanes.

All of my family, even my 7-month-old grandson, now have new flashlights and fresh new batteries. Government leaders on every level now have a better understanding of technology, management issues and are aware of the importance of cooperation between local, State and Federal officials. What is more, the millennium bug provided a reason to upgrade government technology systems and to inventory resources.

So just being able to say some 3 weeks after the year 2000 rollover, it turned out to be a positive experience, that is a testament to the hard work of the House Y2K task force and to the leadership of Chairman Horn and Chairman Morella, and it is also a testament to the efforts of today's witnesses, particularly Mr. Koskinen and Mr. Willemssen and the others at the General Accounting Office. Your work over the last—at least 3 years in raising awareness and highlighting the potential problems related to the Y2K date change is to be recognized and commended.

I don't want to leave you with the impression that Y2K glitches didn't occur. In fact, at least one bank in my home State of Illinois did experience some Y2K problems when it was temporarily unable to make some Medicare transactions. The Federal Government, I don't think, was immune either. Three of the Federal Housing Administration mission-critical systems experienced problems shortly after January 1st.

So we are here today really, I think, to see if there are any outstanding Y2K issues and to sort out what went right and what

went wrong, and to help the American people understand what transpired on January 1, 2000, and let them know about the significant long-term benefits this situation provided to our government and to private industry.

So, again, I commend the men for calling the hearing today and for all the work you have both done on this important issue and look forward to hearing from the witnesses. Thank you.

[The prepared statement of Hon. Judy Biggert follows:]

JUDY BIGGERT
13TH DISTRICT, ILLINOIS

COMMITTEES:
BANKING AND FINANCIAL SERVICES
GOVERNMENT REFORM
SCIENCE

WASHINGTON, D.C. OFFICE:
508 CANNON HOUSE OFFICE BUILDING
(202) 225-3515
FAX (202) 225-9420

ILLINOIS OFFICE:
115 W. 55TH STREET
SUITE 100
CLARENDON HILLS, IL 60514
(630) 655-2052
FAX (630) 655-1061

Congress of the United States
House of Representatives
Washington, DC 20515–1313

Opening Statement of Representative Judy Biggert (R-IL)
Government Reform Subcommittee on Government Management, Information & Technology
Hearing on the Year 2000 Computer Problem: What Did We Learn
January 27, 2000

Good morning, Chairman Horn and Chairwoman Morella. Let me start by welcoming everyone back and wishing you all a happy and productive year. Let me also thank you for calling this hearing on the impact of the Year 2000 date change.

26 days have passed since the arrival of the Year 2000. I am pleased to note that the world didn't come crashing down around us. Almost as important, at least for the members of this haggard Task Force, the dawning of the new year showed us that the Y2K bug didn't have a serious bite.

Contrary to what some felt might happen, planes didn't fall from the sky when the clock struck midnight on January 1, 2000. Telephones retained their dial tone, water still ran from the faucets and America's New Year celebrations were not left in the dark.

Remarkably and perhaps a bit surprisingly, substantial Y2K problems were not experienced outside of this country either. Despite the total lack of preparation on the part of some nations, computer and other essential services across the globe saw no major disruptions.

In retrospect, I believe the Y2K bug proved to be more beneficial than it was harmful. Yes, some could argue that the billions of dollars spent in this country and elsewhere to combat Y2K problems were frittered away. Some could also argue that concerns expressed about the date rollover where overblown. But, I don't agree.

As this Committee heard numerous times during its hearings on the Year 2000 issue, Y2K related glitches could have had both a substantial and extremely negative impact on a variety of services. The smooth turnover from 1999 into 2000 is directly related to the billions of dollars and hundreds of man-hours directed toward preventing and correcting potential Y2K problems. I think it goes without saying that from what we have seen – or have not seen thus far – relating to Y2K disruptions that these efforts paid off handsomely.

Y2K preparations paid off in other ways as well. As a result of Y2K concerns, there are now thousands more American families that own the equipment, such as generators, needed to prepare for other types of emergencies, namely snow storms, floods and hurricanes.

Government leaders on every level now have a better understanding of technology management issues, and are aware of the importance of cooperation between local, state and federal officials. What's more, the millennium bug provided a reason to upgrade government technology systems and to inventory resources.

Just being able to say some three weeks after the Year 2000 rollover that it turned out to be a positive experience is a testament to the hard work of the House Y2K Task Force and to the leadership of Chairman Horn and Morella. It is also a testament to the efforts of today's witnesses, particularly Mr. Koskinen, who served as Chair of the President's Council on the Year 2000 Conversion, and to Mr. Willemssen and others at the General Accounting Office (GAO).

Your work over the last three years in raising awareness of and highlighting potential problems relating to the Year 2000 date change is to be recognized and commended.

I don't want to leave you with the impression that Y2K-glitches did not occur. In fact, at least one bank in my home state of Illinois experienced Y2K problems when it was temporarily unable to make Medicare transactions. The federal government was not immune from these problems either. Three of the Federal Housing Administration's mission-critical systems experienced problems shortly after January 1st.

And this is why we are here today – to work through the outstanding Y2K issues and to sort out what went right and what went wrong with our Y2K preparations. We are here to help the American people understand what transpired on January 1, 2000 and to let them know about the significant long-term benefits this situation provided to our government and to private industry.

Again, Mr. and Madam Chairman, I commend you for calling this hearing and for all the work you have done on this important issue. I look forward to hearing from our witnesses and thank them for joining us today.

Thank you.

Mr. HORN. Well, thank you very much. I now yield to the gentleman from Oregon, Mr. Walden, who has been with us in field hearings and a faithful worker in the very active work of these subcommittees. Mr. Walden, the gentleman from Oregon.

Mr. WALDEN. Thank you very much, Mr. Chairman. I want to extend my appreciation to the work you have done and others on this committee certainly for bird-dogging this issue throughout the last year or more. I think in large measure, the report cards that you issued were a very positive step in not only notifying our own agencies, but the world, where we stood and proved to be a very effective technique for spurring on the changes that needed to be made to cope with the Y2K issue.

In my other life, I was a small business owner, and I can tell you Y2K was not a cheap thing to go through. Our own little company spent well over $40,000 in upgrading software. I know that I am not alone in the small business community in that respect. So there was an enormous amount of capital spent to deal with this issue, and hopefully the programmers who will deal with the 10K issue, I won't have to help pay for them down the road.

But I think it was an excellent exercise. I think it forced both of us in both the government and private industry to do an incredible amount of improvement to our software and to our hardware. That should help us down the road in a competitive status as well.

So, Mr. Chairman, I again want to thank you for your tireless efforts to make that the country was ready, and I look forward to hearing from our panelists as well. Thank you.

Mr. HORN. I thank the gentleman for your kindness.

The next gentleman has also been very active since he has come here in the last election, Mr. Green of Wisconsin, Mark Green. He has been faithfully working on some of these problems and has a whole series of other things he wants us to consider too, and we will.

Mr. GREEN. Thank you, Mr. Chairman. I have no comments at this time, but will look forward to the testimony.

Mr. HORN. Thank you very much.

Now it is a great pleasure to present the person that put the executive branch together, where it was no question it wasn't going anywhere until the President picked Mr. Koskinen out of retirement, who delayed his trip to France to have time for retirement after his position as Deputy Director for Management of the Office of Management and Budget. You did a great job, John, and we are delighted to have you here with your thoughts as to what happened and what did we learn from it, and what can we use from it.

STATEMENTS OF JOHN KOSKINEN, ASSISTANT TO THE PRESIDENT, CHAIRMAN, PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION; JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE; CHARLES ROSSOTTI, COMMISSIONER, INTERNAL REVENUE SERVICE; AND FERNANDO BURBANO, CHIEF INFORMATION OFFICER, DEPARTMENT OF STATE

Mr. KOSKINEN. Thank you, Mr. Chairman. Good morning. I am pleased to appear once again before this joint session of the subcommittees to discuss the activities of the President's Council on

Year 2000 Conversion and the Nation's successful transition to the year 2000. With your permission, I will submit my full statement to the record and summarize it here. I appreciate everyone's kind comments and would like to acknowledge as well the work of your subcommittees in helping to prepare the Federal Government and the country for the century date change.

I appreciate your work and I think it deserves recognition as we look back on what has been truly a remarkable effort.

I continued to believe that Y2K was the greatest management challenge the world has faced in the last 50 years. Given the size of the task, it is easy to understand why just 2 or 3 years ago many serious people who had looked at the situation maintained there was no way the work could be finished in time. When I returned to the government in March 1998 to work on Y2K, things were fairly grim. The consensus was the government wouldn't make it. In the private sector, information bottlenecks were widespread and companies weren't saying much about their own readiness for Y2K.

On top of all that, the World Bank released a study showing that three-quarters of the world's countries had no Y2K plans at all. In short, Y2K looked too mammoth, too complicated and too interconnected to be solvable. Now, almost 2 years later, the United States and much of the world have made the transition into the year 2000 with few problems that have had a noticeable impact on the general public.

How did it hatch? It wasn't by accident. There was a tremendous mobilization of people and resources to make sure that systems would operate effectively into the year 2000. Domestically, participants in key infrastructure sectors, such as electric power, telecommunications finance and transportation devoted great attention and resources to the problem, and as we moved to the ends of the year, operators of systems in those areas stated they were basically done with their Y2K work.

We reported this information in our last quarterly assessment, and, as we expected, there were no major infrastructure failures, nationally or regionally in the United States. The Federal Government was also ready for the year 2000. Two weeks before the new year, 99.9 percent of the government's more than 6,000 mission-critical systems were Y2K ready.

The result was that while it has been noted there have been some glitches, thus far Y2K issues have not affected the major government services and benefits provided to the American people.

Internationally, after a slow start, countries made a concerted effort to ensure that critical issues would be ready for the date change and, as a general matter, major infrastructure systems abroad functioned smoothly during the rollover.

There is general agreement that the Y2K transition went more smoothly than any of us would have imagined. In fact, as noted in the week since the rollover, some people have suggested that Y2K was an insignificant problem, hyped by the media, computer consultants and those with other reasons for hoping the world as we know it was about to end.

The short answer is that I don't know of a single person working on Y2K who thinks that they did not confront and avoid a major risk of systemic failure. Indeed, some of the noteworthy problems

we have seen from difficulties at State motor vehicle offices to credit card processing problems to its Defense Department satellite system failure, proved that Y2K was a very real threat indeed.

While I do not think that the significance of the Y2K problems was exaggerated, there were those who disagreed with our reports indicating that the problem was being successfully addressed. This form of hype can be traced to the skepticism and disbelief in some quarters that companies or governments reporting on their own progress could be telling the truth. In the United States, I kept reminding my doomsayer friends that it made no sense to discount these reports, since everyone who was in a position of responsibility would be easily found after January 1. Many continued to assume the worst would materialize, some now discounting the significance of the Y2K threat point to the relative lack of major disruptions abroad.

How did countries that appeared to have spent so little and were thought to be relatively unprepared emerge unscathed? Here, I think, there were a number of factors at work. Chief among them was the difficulty of getting accurate status reports, especially internationally on a fast-moving issue such as Y2K. Information 3 months old was out-of-date. But in the absence of additional details, people often relied on that older information, and then were surprised when it turned out to have been overtaken by subsequent progress.

Additionally, once you get beyond the world's largest users of information technology, countries like the United States, Canada, Japan and the United Kingdom, the reliance upon information technology drops off quickly. Furthermore, the technology being used in other countries is more likely to be off the shelf and not customized applications that are more difficult to fix.

Finally, countries starting later had the benefits of the lessons learned by those working on Y2K for several years. We spent a lot of time in the last 12 months encouraging the sharing of technical information about problems, products, fixes and testing techniques, and I think it is obvious that worked paid off.

So what lessons can we draw from the Y2K experience? First, Y2K has taught us that top management needs to be more involved in information technology on an ongoing basis, since information technology cuts to the very heart of how organizations conduct their business. In many companies, it was only when the board of directors or the chief executive officer took ownership of the problem that we could see the first signs of any real progress.

Y2K has also shown us that we need to do a better job of configuration management, in other words, keeping track of the technology we use and the functions it performs. Y2K provided many large firms a reason to conduct, for the first time ever, a comprehensive inventory of their information technology infrastructure and processes.

Not surprisingly, organizations found that some systems could be discarded without any loss in productivity. Other systems were replaced by newer, more efficient models. Third, Y2K has demonstrated the value of forming partnerships across traditional boundaries to achieve a common goal. In addition to showing us the increasing interconnectedness of organizations through tech-

nology, Y2K highlighted the fact that private industry and government can work together to address major national issues.

I think that spirit of partnership obviously extended to the political arena as well. Most people realized early on there was not a Democratic or Republican solution to this problem, and we really have worked well together, particularly in the partnership that led to the passage of the Year 2000 Information Readiness and Disclosure Act in 1998.

Finally, I think that Y2K has demonstrated that we need to include the American public in the discussions about any future large-scale challenges. Given the facts, whatever they are, people generally responded appropriately. Even when industry and government information provided to the public revealed that there was still substantial work left to do, people were reassured rather than alarmed. They seemed comforted to know their organizations were treating the problem seriously, were working together to solve it, and would keep them informed with the status of the situation.

The President's Council will soon cease its operations. Before we post the going-out-of-business sign, we will focus on monitoring activities during the leap year rollover. We do not expect any major national problems and we anticipate the Council will shut down for good by the end of March.

In closing, I would like to echo the comments made that the Federal Government and the country's successful resolution of the Y2K problem attributes to the skill, dedication and hard work of thousands of professionals that have focused on this issue. It has been my pleasure to assist them as part of this vital national effort, and I look forward to answering any questions you may have at the conclusion of the other statements.

Mr. HORN. Thank you very much.

[The prepared statement of Mr. Koskinen follows:]

STATEMENT OF JOHN A. KOSKINEN
CHAIRMAN
PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

January 27, 2000

Good morning. I am pleased to appear once again before this joint session of the subcommittees to discuss the activities of the President's Council on Year 2000 Conversion and the nation's successful transition into the Year 2000.

Before moving into the core of my remarks, I would like to acknowledge the work of your subcommittees in helping to prepare the Federal Government -- and the country -- for the century date change. I have told agency employees working on Y2K that the accolades belong to all of those who were part of this unprecedented experience. These subcommittees are no exception. Through oversight and regional hearings, you have played an important role in underscoring the need to address all facets of this important challenge. The result was increased visibility for Y2K and an important stimulus to prompt organizations across the country to prepare key systems for the date rollover. I appreciate your work, and I think it deserves recognition as we look back on what has been a truly remarkable effort.

Today I'd like to discuss some of the more important aspects of how we met the Year 2000 challenge and what the experience can teach us for the future.

The Scope of Y2K

I continue to believe that Y2K was the greatest management challenge the world has faced in the last 50 years. Although the mechanics involved in making a single computer system ready for the Year 2000 were fairly straightforward, the scope of the work was daunting. It involved identifying, fixing, and testing millions of systems and data exchanges in what is truly a global economy. Given the size of the task, it's easy to understand why just two or three years ago many serious people who had looked at the situation maintained there was no way the work could be finished in time.

Several obstacles appeared to confirm that view. There was procrastination. With years to do the work and the possibility that someone would invent a "magic bullet," there were some who questioned the need for prompt action. There was also the perception that Y2K was solely an information technology issue, not a core management problem. As a result, in many organizations, it was just another project battling for scarce financial and management resources on the IT side of the ledger. And there were also serious barriers to cooperation on Y2K in the private sector. Anti-trust issues and a natural tendency to compete for advantage made working together on Y2K difficult, if not inconceivable, for many companies.

Thus, when I came back to the government in March 1998 to work on Y2K, things were fairly grim. Chairman Horn had just given the Federal agencies a grade of "D- minus" for their efforts to prepare systems for the Year 2000. In the interest of full disclosure I should note that, after three months of my leadership, the grade changed -- to an "F." The consensus was that the Government wouldn't make it. The FAA, the IRS, the Health Care Financing Administration, and the Defense Department were all thought to be lost causes. Some were predicting that there was a significant chance that government agency failures alone would send the economy into a deep recession.

In the private sector, information bottlenecks were widespread. Everyone worried that they would be sued for anything they said about the compliance of products or devices they used, or their test processes and results. And companies also weren't saying much about their own readiness for Y2K. Thus, their business partners – as well as the general public -- assumed the worst. The mantra for much of 1998 was "we think we'll be all right, but we have no confidence in our suppliers and utility providers."

On top of all that, the World Bank released a study showing that three-fourths of the world's countries had no Y2K plans. And the fabled 50 billion embedded chips operating in everything from microwave ovens to airplanes to drilling rigs in the North Sea were becoming the growth industry of the problem, since many organizations had been focusing on fixing software and not hardware or operating systems.

In short, Y2K looked too mammoth, too complicated, and too interconnected to be solvable. But that was then.

Meeting the Challenge

Now, almost two years later, the United States and much of the world have made the transition into the Year 2000. Thus far, there have been few problems that have had a noticeable impact on the general public. How did it happen? It wasn't by accident. There was a tremendous mobilization of people and resources to make sure that systems would operate effectively into the Year 2000. In the United States alone, the Commerce Department estimates that the total bill for Y2K efforts among business and government will exceed $100 billion.

Domestically, participants in key infrastructure sectors such as electric power, telecommunications, finance, and transportation devoted a great deal of attention to the problem. As we moved toward the end of the year, operators of systems in these areas stated they were basically done with their Y2K work. We reported this information in our last quarterly assessment and the result was that, as we expected, there were no major infrastructure failures – nationally or regionally -- in the United States. The lights stayed on, the phones and ATMs worked, and rail, transit and air transport systems functioned normally.

Government was ready for the Year 2000 as well. Thanks in large part to the hard work of thousands of dedicated public servants, the Federal Government made dramatic strides toward Y2K readiness in the two years leading up to the transition. Two weeks before the New Year, 99.9 percent of the Government's more than 6,000 mission-critical systems were Y2K ready. Agencies had also been conducting thorough end-to-end tests with States and other partners for key programs that have a significant impact on the public, including unemployment insurance, Medicaid and Food Stamps. The result was that, while there were some glitches, thus far Y2K issues have not affected the major government services and benefits provided to the American people.

It is worth noting that, in both government and the private sector, organizations understood the value of contingency plans in making sure that, if Y2K-related failures did occur, these failures would not force work to grind to a halt. Businesses and governments formulated or updated contingency plans and strategies to allow them to continue their most important functions in the event of Y2K problems. The result was that, when glitches surfaced, most organizations were able to rely upon back up processes as they worked to restore normal operations. Since most problems were fixed very quickly, most customers and constituents were not seriously inconvenienced and, in most cases, were unaware of the difficulties.

Internationally, after a slow start, countries made a concerted effort to ensure that critical systems would be ready for the date change. For example, when we gathered people together at the United Nations in December 1998, 120 countries sent delegates, probably half of whom weren't sure why they were there. By the time we reassembled them last June, 173 countries sent delegates to what was the largest meeting for a special purpose in UN history. Not one of those countries thought Y2K was not an important problem for them. By then, most had participated in at least two meetings in their continental regions designed to share Y2K information in critical areas such as power, telecommunications and transportation. As a general matter, major infrastructure systems abroad functioned smoothly during the rollover. Financial markets around the world, which were closely monitored, conducted normal operations in business days after January 1. To date, there have been no reports of serious Y2K-related problems that have affected trade between the United States and its major economic partners.

Outstanding Questions

There is general agreement that the Year 2000 transition went more smoothly than any of us would have imagined. Some even noted that the positive outcome made it look too easy. Indeed, the results of our efforts have prompted some interesting questions that I would like to address here today.

In the weeks since the rollover, some people have said Y2K was an insignificant problem hyped by the media, computer consultants and those with other reasons for hoping the world as we know it was about to end. Doubt has been expressed about the reality of the problem and the necessity for the significant investment of time and money to avoid disruptions. The short answer is that I don't know of a single person working on Y2K in a major bank, financial institution, telephone company, electric power company or airline who thinks they did not confront -- and avoid -- a major risk of systemic failure. Indeed, some of the noteworthy problems we have seen – from difficulties at State motor vehicle offices to credit card processing problems to the Defense Department satellite system failure – prove that Y2K was a very real threat indeed.

While I do not think that the significance of the Y2K problem was exaggerated, there were those who disagreed with our reports indicating that the problem was being successfully addressed. This "hype" can be traced to the skepticism and disbelief in some quarters that companies or governments reporting on their own progress couldn't be telling the truth. In the U.S., I kept reminding my doomsayer friends that it made no sense to discount these reports since everyone in a position of responsibility would be easily found after January 1 and held accountable if they had misrepresented the situation and their systems failed. We were not just managing to December 31. We were managing through the rollover. But many continued to assume the worst would materialize even as much of the self-reporting indicated, accurately it turns out, that we were going to make the transition into the new millennium successfully.

Some discounting the significance of the Y2K threat point to the relative lack of major disruptions abroad. How did countries that appeared to have spent so little and were thought to be relatively unprepared emerge unscathed? Here, I think that here there were a number of factors at work. Chief among them was the difficulty of getting accurate status reports – especially internationally -- on a fast moving issue such as Y2K. Information three months old was out of date. But in the absence of additional details, people often relied on that older information and then were surprised when it turned out to have been overtaken by subsequent progress. A report about risks from April or June was assumed to still be operative in October. In many cases, what was missed was the fact that, while some countries spent less, they may have spent the bulk of their funds in a concentrated effort the last six to nine months of 1999.

Additionally, once you get beyond the world's largest users of information technology – countries like the U.S., Canada, Japan and the United Kingdom -- the reliance upon IT drops off

quickly. In many of these less IT-focused countries, there were other factors at work that made for an easier transition into the Year 2000. The technology being used is more likely to be "off the shelf," not customized. Also, unlike the United States, countries like Spain and Italy that have moved into IT more recently were not saddled with old legacy systems built with antiquated, customized code by people who had long since retired. The bottom line is that the fixes were frequently more straightforward in those countries than in the U.S.

Finally, countries starting later had the benefit of the lessons learned by those who had been working on Y2K for several years. We spent a lot of time in the last 12 months encouraging the sharing of technical information about problems, products, fixes and testing techniques. I think it's obvious that work paid off. Elevators provide a good example. Two years ago everyone was testing to see if the elevator-specific systems were a problem. Once it was learned that they were not, no one else had to spend time pursuing that issue. Similar experiences took place in industries like banking, finance, telecommunications, air traffic and electric power, where information was being exchanged and shared globally in a way never seen before.

Small business was another area about which many, including the Council, had voiced concerns. While there were relatively few reports of Y2K-related failures among small businesses, many glitches were just fixed without any further discussion. Similar to our experience before the rollover in trying to gather status information for small businesses, I think the sheer numbers of these companies and the lack of standard reporting relationships make it just as difficult to discover how many small businesses actually had Y2K difficulties. Furthermore, I think that for firms large and small there is a natural inclination not to report items that are fixed in very short time frames. A business may have suffered a Y2K glitch, but if they were able to fix it in a few hours and no one was affected – why report it? This phenomenon was revealed before the rollover when surveys showed that over 70 percent of companies reported they had experienced Y2K glitches. Doomsayers noted that this indicated the pervasive nature of the Y2K problem. We noted that it demonstrated most Y2K problems could be fixed without anyone noticing.

Moving Forward

So what lessons can we draw from the Y2K experience? I think there are some important principles we need to carry with us as we move forward.

First, Y2K has taught us that top management needs to be more involved in information technology on an ongoing basis since IT cuts to the very heart of how organizations conduct their business. In many companies, it was only when the Board of Directors or the CEO took ownership of the problem that we could see the first signs of any real progress. It became clear that only senior management could make Y2K a top priority at the expense of other IT projects.

For example, upon my return to government I announced that I would begin to attend the monthly senior management meetings of agencies facing the greatest Y2K challenges. This was partially to ensure that they were holding such meetings. Some were not. At the Vice President's suggestion, he and I also met with the Cabinet officers from those agencies in September 1998. We asked them to discuss the impediments to their making better progress and to commit to whatever steps were necessary to make it over the hurdles.

The major difficulty for many of these agencies was their need to complete other high-priority IT projects. The consensus of this discussion was that there was no higher priority than to have systems function properly into and through the Year 2000. The only person who could enforce that view was the agency head. The same concept applies as organizations confront ongoing challenges about how to harness the potential of information technology to improve their operations in other areas.

Y2K has also shown us that we need to do a better job of "configuration management" – in other words, keeping track of the technology we use and the functions it performs. Y2K provided many large firms a reason to conduct – for the first time ever -- a comprehensive inventory of their information technology infrastructure and processes. That was certainly true for the Federal Government. Not surprisingly, organizations found that some systems could be discarded without any loss in productivity. Other systems were replaced by newer, more efficient models. And wildly inconsistent systems and processes were found to be just what they are -- impediments to efficient operations. At the same time, we have come face to face with the costs of sloppy software development and inconsistent or nonexistent standards. We need to do better in the future.

Third, Y2K has demonstrated the value of forming partnerships across traditional boundaries to achieve a common goal. In addition to showing us the increasing interconnectedness of organizations through technology, Y2K highlighted the fact that private industry and government can work together to address major national issues. Through our numerous industry working groups, the President's Council was able to bring key industries together to increase the level of Y2K awareness and activity and, in several cases, to set industry benchmarks for completing Y2K work. In addition, the industry surveys undertaken at our request played a critical role in prodding laggard companies to match the progress of their peers.

I think that spirit of partnership extended to the political arena as well. Most people realized early on that there was not a Democratic or Republican solution to this problem. We really have worked together. The Year 2000 Information and Readiness and Disclosure Act passed in the fall of 1998 by the Congress at our request broke the logjam on information sharing and led to more disclosures about readiness and experiences with individual products and fixes. It was critical legislation, and the odds were stacked against it given the limited time remaining in the session and the need for unanimous consent, without hearings. But the bill passed, and the President signed it into law. The challenge for all of us is to build on these partnerships as we

deal with future challenges to our information technology infrastructure.

Y2K has helped us all to develop a better appreciation of our growing reliance on information technology. This increased awareness should encourage all of us to devote more time and resources to improving and protecting these systems. But we also need to look more closely at the widening gap between the IT "haves" and "have nots." If we are to truly move into the 21st century on the wings of electronic commerce, we need to focus our energies on finding ways to bring others who lack IT -- domestically and internationally -- along with us.

Finally, I think that Y2K has demonstrated that we need to include the American public in the discussions about any future large-scale challenges. Eighteen months ago, most polls showed that many people were extremely anxious about Y2K. Sales of survival food and equipment were going off the charts. I believed then, as I do now, that people are more inclined to panic when they don't have information and when they think that the system is out of control. Given the facts, whatever they are, people generally respond appropriately. Even when industry and government information provided to the public revealed that there was still substantial work left to do, people were reassured, rather than alarmed. They seemed comforted to know that organizations were treating the problem seriously, were working together to solve it, and would keep them informed about the status of the situation. The dialogue with the public continued throughout 1999, aided by our campaign to encourage "community conversations" about Y2K. The net result was that we didn't see a noticeable overreaction by the public, even during the time of increasing focus on the impending transition to the New Year.

In fact, the public seems to have gotten it just right. They were anxious about the problem in 1998, grew more confident throughout 1999, and now seem pleased that there were no major difficulties and that they can continue on with their lives.

Signing Off

The President's Council will soon cease its operations. But before we post the "going out of business" sign, we will be focused on monitoring activities during the Leap Year rollover. So we will operate the Information Coordination Center once again with detailees from the Federal agencies to collect information on key Federal, State and private sector systems during the period from February 28 through March 1. While the leap year rollover is unlikely to affect hardware or operating systems, it could pose a significant challenge to software applications in which programmers did not account for the extra day in the Year 2000.

Nonetheless, we do not expect any major, national problems and we anticipate that the Council will shut down for good by the end of March. In closing, I would like to say that the Federal Government and the country's successful resolution of the Y2K problem is a tribute to the skill, dedication, and hard work of thousands of professionals that have been focused on this issue. It has been my pleasure to assist them as part of this vital national effort.

Mr. HORN. We will go down, as you know, with this panel and then open it up to questions, because I think some of the information will jibe and some won't.

The gentleman from the General Accounting Office, Mr. Joel Willemssen, the Director of Civil Agencies Information Systems, Accounting and Information Management Division. Mr. Willemssen has gone all over the United States with the subcommittee on government management and has been an active participant in the various panels we have had of government officials, private sector and so on. So it is a pleasure to have you here.

I know you were working right up to midnight there, as I saw you in John's command center. So we appreciate all you have done and your team at the General Accounting Office.

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Chairwoman Morella, Ranking Member Turner, members of the subcommittees, thank you for inviting us to testify today. As requested, I will summarize our statement.

Overall, during the rollover period, our country had relatively few Y2K-related errors that affected the delivery of key services. While the Y2K challenge is not yet over, because some key business processes have not yet been fully executed and some risky dates remain, the Nation's success thus far is a very positive indicator that these hurdles will also be overcome. The leadership exhibited by the legislative and the executive branches and the partnerships formed by numerous organizations were pivotal factors behind the success.

The Y2K-related errors that were experienced during the rollover generally did not affect the delivery of key services because they were either corrected quickly or contingency plans were implemented. A key reason that Y2K errors had little effect on the delivery of services is that Federal agencies and other organizations used the rollover weekend to identify and correct errors before the problems resulted in operational consequences.

In the Federal Government, the few Y2K disruptions that were significant were mitigated by quick action. For example, the Department of Defense, Health Care Financing Administration and Federal Aviation Administration each experienced significant Y2K events that they were able to address quickly.

For high impact State-administered problems such as Medicaid, food stamps and unemployment insurance, actions by States and the Federal Departments of Agriculture, Health and Human Services and Labor have paid off. Errors reported were often cosmetic printing or display problems with few failures resulting in disruptions to service.

The threat posed by Y2K was a much needed wake-up call for organizations to improve their management of information technology. Y2K has laid a foundation for longer term improvements in the way that Federal Government manages information technology. I would like to quickly summarize some of the key lessons that we have learned out of the Y2K experience.

First, as mentioned, one of the most important factors underpinning the success of Y2K was leadership at the highest levels of government. In particular, congressional oversight played a central

role in pushing agencies forward on Y2K. Mr. Koskinen and the President's Y2K Council provided strong effective leadership.

Second, Y2K served as a notice to many on how much we rely on information technology to deliver key services.

Third, there was standard guidance that was put together that was universally accepted, adopted and implemented, which facilitated Y2K efforts and oversight. Such guidance provided consistency, imposed structure and discipline and enhanced the rigor of testing and assessment efforts.

Fourth, as Mr. Koskinen mentioned, the establishment of partnerships among various organizations was especially important. In particular, the partnerships formed by Mr. Koskinen, Federal agencies and private sector organizations were instrumental to the Nation's Y2K efforts.

Fifth, we found that using standard techniques and metrics to monitor performance was especially helpful in measuring progress and remaining challenges.

Finally, Y2K saw many agencies take charge of their information technology resources in much more active ways. In many instances, it forced agencies to inventory their systems and to link those systems to agencies' core business processes. Also the development and testing of contingency plans should have benefits way beyond Y2K.

Further, Y2K prompted agencies to establish needed policies in areas such as configuration management, risk management and software testing.

In summary, the Y2K rollover was clearly a success for our Nation. A key challenge now for the Federal Government is ensuring that the lessons learned in addressing Y2K can be effectively used to improve overall information technology management.

That concludes the summary of my statement. Thank you very much.

Mr. HORN. I thank you very much. We have a lot to pursue in your very fine document here as to what did go wrong.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform and the Subcommittee on Technology, Committee on Science, House of Representatives

YEAR 2000 COMPUTING CHALLENGE

For Release on Delivery
Expected at
10 a.m. EST
Thursday,
January 27, 2000

Leadership and Partnerships Result in Limited Rollover Disruptions

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-70

Mr. Chairman, Ms. Chairwoman, and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on the change of century rollover. According to the report of the President's Commission on Critical Infrastructure Protection, the United States—with close to half of all computer capacity and 60 percent of Internet assets—is the world's most advanced and most dependent user of information technology.[1] Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. As a result, the United States was particularly at risk that system failures resulting from the change of century rollover would have adverse consequences on the public.

At this time, federal, state, and local governments as well as key sectors report that they have successfully met the Year 2000 challenge. While Year 2000 failures have occurred—some significant but most considered minor—these entities report that almost all of these failures have been mitigated, either through the correction of systems or by the implementation of contingency actions. Accordingly, few Year 2000 failures have adversely affected the public. While the Year 2000 challenge is not yet over because some key business processes have not yet been fully executed and because other risky dates remain, the nation's success thus far is a very positive indicator that these hurdles will also be overcome. The leadership exhibited by the legislative and executive branches and the partnerships formed by a myriad of organizations were pivotal factors behind this success. Ensuring that the lessons learned in addressing the year 2000 are effectively used to improve information technology management is a key challenge now facing the federal government.

---

[1] *Critical Foundations: Protecting America's Infrastructures* (President's Commission on Critical Infrastructure Protection, October 1997).

After providing brief background information, today I will discuss (1) the reporting structure established by the government to obtain information on Year 2000-related failures during the rollover period, (2) examples of Year 2000 errors and their resolution, and (3) lessons from the Year 2000 effort that can be carried forward to improve the management of information technology activities. Appendix I provides our objectives, scope, and methodology.

BACKGROUND

Because of its urgent nature and the potentially devastating impact it could have had on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[2] Since that time, we have issued over 160 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

The public faced the risk that critical services provided by the government and the private sector could be disrupted by the change of century rollover. As we have previously testified, financial transactions could have been delayed, flights grounded, power lost, and national defense

[2] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1997).
[3] These publications can be obtained through GAO's World Wide Web page at *www.gao.gov/y2kr.htm*.
[4] *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997); *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998); *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998); and *Y2K Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22, issued as a discussion draft in September 1999 and in final form in October 1999).

affected.[5] Fortunately, as we testified before your Subcommittees in November 1999,[6] at the urging of congressional leaders and others, the Office of Management and Budget (OMB) and federal agencies dramatically increased the amount of attention and oversight given to the Year 2000 issue.

Most importantly, on February 4, 1998, the President signed an executive order that established the President's Council on Year 2000 Conversion, chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies; (2) acting as chief spokesperson in national and international forums; (3) providing policy coordination of executive branch activities with state, local, and tribal governments; and (4) promoting appropriate federal roles with respect to private-sector activities. The council focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community.

Among the many initiatives undertaken by the government, which improved its own as well as the nation's preparedness, were the following:

- On March 26, 1999 OMB implemented our April 1998 recommendation that governmentwide

[5] *Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions* (GAO/T-AIMD-98-262, August 13, 1998).
[6] *Year 2000 Computing Challenge: Noteworthy Improvements in Readiness But Vulnerabilities Remain* (GAO/T-AIMD-00-37, November 4, 1999).

priorities be set by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery; OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; and assuring that each partner had an adequate Year 2000 plan and, if not, helping each partner without one.

- OMB clarified its contingency plan instructions and, along with the Chief Information Officers Council, adopted our business continuity and contingency planning guide for federal use. In addition, on May 13, 1999 OMB required agencies to submit high-level versions of these plans.

- Council officials participated in monthly, multistate conference calls with state Year 2000 coordinators. The latest of these calls occurred on January 3; 36 states participated and discussed the results of the century rollover. Moreover, in July 1998, March 1999, and October 1999, the Council—in partnership with the National Governors' Association—convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.

- The Council established a nationwide campaign to promote "Y2K Community Conversations" to support and encourage the efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the

[4] *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships* (GAO/AIMD-98-85, April 30, 1998).

Council developed a toolkit that provided examples of which sectors should be represented at these events, and issues that should be addressed.

- The Council established over 25 sector-based working groups and conducted outreach activities, likewise consistent with our April 1998 recommendation.[8] Also consistent with an April 1998 recommendation, the Chair directed the Council's sector working groups to assess their sectors. In 1999, the Council subsequently issued four public reports summarizing these assessments.

We testified before you in November 1999 that as a result of these efforts substantial progress had been made to reduce the risk posed by the Year 2000 problem.[9]

INFORMATION COORDINATION CENTER ESTABLISHED TO MONITOR AND ASSESS ROLLOVER PERIOD

On June 14, 1999, the President created the Information Coordination Center (ICC) to assist the Chair of the President's Council on Year 2000 Conversion. The ICC was charged with making preparations for information-sharing and coordination within the federal government and key components of the public and private sectors, coordinating agency assessments of Year 2000 emergencies and, if necessary, assisting federal agencies and the Chair of the Council in reconstituting processes. Accordingly, under the umbrella of the ICC, the federal government

[8] *GAO/AIMD-98-85, April 30, 1998.*
[9] *GAO/T-AIMD-00-37, November 4, 1999.*

implemented a large-scale reporting process to obtain information on events occurring during the rollover weekend from major federal agencies, states, key sectors, and foreign countries.

ICC Reporting Process Structured to Obtain Selected Status Information From Federal Agencies, State and Local Governments, Key Sectors, and Foreign Countries

To obtain information from a variety of sources, including federal agencies, states, localities, and key sectors, an ICC contractor developed an unclassified reporting system, the Information Collection and Reporting System (ICRS), which was used by these entities to provide status and incident information to the ICC and others. Reporting entities were to provide status information to ICRS through a series of organization-specific input screens. If an incident occurred during the reporting period, whether Year 2000-related or not, the reporting entity was responsible for determining whether the situation was still normal ("green" status), or whether the incident had resulted in reduced capacity, capability or service ("yellow" status), or significantly reduced capacity ("red" status). The ICC directed all reporting entities to provide reports twice a day and/or whenever a significant change in status occurred between December 28, 1999, and January 7, 2000.

Each of the 24 major departments and agencies except for the Departments of Defense and State reported on their status during the rollover period using ICRS. Defense provided classified status information via a secured telecommunications line to the ICC's Sensitive Compartmented Information Facility. State provided the ICC with verbal reports and provided access to its Weathervane system in the Sensitive Compartmented Information Facility. The Weathervane system provided each embassy's assessment of the status of its foreign country.

The Federal Emergency Management Agency (FEMA) was the primary liaison for gathering information from state and local governments. FEMA used its 10 Regional Operation Centers—interim command and control sites that can be activated to monitor potential disasters such as hurricanes—to monitor the rollover to the year 2000. From December 28, 1999, through January 4, 2000, the Regional Operations Centers responsibilities included (1) reviewing states' ICRS Y2K status reports, (2) contacting states that did not submit reports and obtaining the state's Y2K status, (3) preparing and submitting regional ICRS Y2K status reports to FEMA headquarters, and (4) participating in daily teleconference calls with FEMA headquarters. If requested, the centers also sent representatives to their respective states' emergency operation centers for the rollover period to provide on-site monitoring of states' Y2K status, and help states request federal assistance if needed. FEMA headquarters was responsible for reviewing and assessing regional input and summarizing national-level information.

Individual states were responsible for designating a point of contact responsible for submitting ICRS reports and determining how local reports would be provided to the ICC. With respect to local reporting, states had the option of using their own reporting mechanism or obtaining and distributing ICRS passwords to localities that would allow them to submit ICRS status reports. According to the ICC, about 670 localities in 37 states submitted ICRS status reports on or after January 1, 2000. States were also responsible for reviewing and assessing locality status information and entering state-level status information. In addition, states were to submit separate reports on the status of federally funded programs, such as food stamps and unemployment insurance.

To obtain status information from key sectors, six federal organizations also worked with private-sector organizations designated as National Information Centers to provide information to the ICC on critical sectors during the rollover period. For example, for the rollover period the Department of Energy implemented an emergency operations center that included representatives from the North American Electric Reliability Council, American Gas Association, American Petroleum Institute, and the Interstate Natural Gas Association of America—each a National Information Center. Along with the Department of Energy, these entities were charged with monitoring reports from the field and performing impact analyses. Both the Department of Energy and the North American Electric Reliability Council periodically submitted ICRS reports. The Department of Energy reported on the status of its mission-critical systems, online computer systems, headquarters building infrastructure, field building structure, operational health/safety systems, federal electric power, electric power, oil, and gas areas. The North American Electric Reliability Council reported on the status of specific electric power organizations. Table 1 lists the sectors that had National Information Coordination Centers, responsible private-sector organizations, and lead federal organizations.

Table 1: National Information Centers

Sector	National Information Center Organization	Lead Federal Organization
Airlines	Air Transport Association	Department of Transportation
Cyber Assurance	Cyber Assurance National Information Center	Information Coordination Center
Electric Power	North American Electric Reliability Council	Department of Energy
Financial Services	Securities Industry Association	Securities and Exchange Commission
Natural Gas	American Gas Association	Department of Energy

Natural Gas	Interstate Natural Gas Association of America	Department of Energy
Oil	American Petroleum Institute	Department of Energy
Pharmaceuticals	National Pharmaceutical Alliance	Department of Health and Human Services
Pharmaceuticals	National Association of Chain Drug Stores	Department of Health and Human Services
Retail	National Retail Federation	Information Coordination Center
Telecommunications	Network Reliability and Interoperability Council	National Communications System

Source: ICC.

To obtain international information, the ICC relied on information provided by the Departments of State, Defense, and Transportation, the National Security Council, and the National Information Centers. In addition, the ICC obtained information from the International Y2K Cooperation Center's[10] Global Status Watch system. This system, developed and operated by an ICC contractor, was used by foreign countries to post information, using a standard template, on the status of major infrastructure areas such as energy, telecommunications, water, and government services. Similar to the ICRS, this system called for countries to report on Year 2000- or non-Year 2000-related events and whether each sector was operating at normal capacity, reduced capacity or service, or significantly reduced capacity or service. During the rollover period, the Chair of the President's Council on Year 2000 Conversion also participated in telephone calls with other national Year 2000 coordinators.

[10]The International Y2K Cooperation Center was created by the United Nations to promote strategic cooperation and action among governments, peoples, and the private sector to minimize adverse Year 2000 effects on the global society and economy.

ICC Gathered and Analyzed Status Information During the Rollover Period

To accomplish the goal of gathering, analyzing, and summarizing information on system operations, the ICC had a core administrative staff that was supplemented during the rollover period with officials detailed from federal agencies. During the rollover period of December 28, 1999, through January 7, 2000, the ICC was organized by sector, each headed by federal agency leads (see table 2).

Table 2: ICC Structure

Sector	Lead Federal Organization(s)
Cyber-assurance	ICC, Critical Infrastructure Assurance Office, and the Federal Computer Incident Response Capability
Financial services	Federal Reserve Board
Small business	Small Business Administration
Chemical related manufacturing	Environmental Protection Agency
Drinking water	Environmental Protection Agency
Hazardous materials	Environmental Protection Agency and the U.S. Coast Guard
Wastewater treatment	Environmental Protection Agency
Emergency services	FEMA
Mission-critical systems	Office of Management and Budget
Public safety	Department of Justice
State & local governments	FEMA
Tribal governments	Department of the Interior
Education	Department of Education
Employment-related protection	Department of Labor
Federal benefits payment programs	Social Security Administration
Food supply	Department of Agriculture
Health care	Department of Health and Human Services
High-impact federal programs	Office of Management and Budget
State-administered federal programs	Office of Management and Budget
National security & international affairs	Departments of Commerce, Defense, and State
Building operations	General Services Administration
Energy	Department of Energy
Communications	Federal Communications Commission/General Services Administration
Transportation	Department of Transportation

Source: ICC.

Sector leads, and their supporting staff, were responsible for maintaining continuous understanding and current status information on their sector during the century rollover period. In performing these duties, they reviewed ICRS status reports, obtained relevant information from their respective organizations through telephone conversations, faxes, and e-mails, and

reviewed media reports. Each sector also provided periodic summaries of its status. These summaries were used to provide status information to the Chair of the President's Council on Year 2000 Conversion as well as to the public.

Since ending full operations on January 7, the ICC discontinued ICRS reporting and directed federal agencies to report on their status daily via e-mail until January 31. The ICC plans to begin full operation again during the leap year rollover between February 28 and March 1.

ICRS Reporting Processes Generally Worked As Expected, But Did Not Capture All Year 2000-Related Incidents

On the basis of our observations, the ICRS reporting processes generally worked as expected. In particular, during the peak reporting times of December 31, 1999 through January 3, 2000, ICC officials and sector leads and supporting staff reviewed and assessed ICRS status reports as well as media reports. Where it was determined to be significant and relevant, they followed up on possible Year 2000-related incidents with their agencies and others. For example, the Small Business Administration representatives at the ICC obtained information from the agency's regional offices on problems being experienced by some small businesses. In some cases, agencies were able to determine that a reported problem was false. In another example, a Department of Health and Human Services representative at the ICC contacted the Food and Drug Administration about a problem with a hospital dispensing system that had been reported on an Internet site. The Food and Drug Administration investigated the reported problem and found it to be false.

Information gathered from these various sources at the ICC was intended to concentrate on events that were the result of system and operational disruptions or that might be impacted by such disruptions. Accordingly, not all Year 2000 incidents were expected to be reported and assessed. At the same time, the Director of the ICC stated that he encouraged entities to use the remarks section in the ICRS to elaborate on other important Year 2000-related incidents. However, he stated that organizations' use of the remarks section was "mixed"—some organizations provided a considerable amount of data on minor anomalies while others had no incidents or elected not to elaborate on any issues that they might have had.

With respect to key sectors, while private-sector representatives in the United States provided information to the ICC, it is not likely that all Year 2000-related errors were reported since the government could not mandate that all incidents be reported. Indeed, on January 3, 2000, the Chair of the President's Council on Year 2000 Conversion stated that "probably some of them [private companies] are having computer glitches and not reporting it to us." He added that if a business is having a minor problem that they were probably not reporting it.

Data limitations were particularly applicable in the international arena. On January 2, 2000, the Chair of the President's Council noted these limitations. He stated that U.S. embassies were not collecting data at the same level as in the United States, and that they did not have the same ability to check with all of the private-sector providers in other countries. The Chair characterized the Department of State's Weathervane system, which captured information from U.S. embassies, as a users' report on whether there were any problems with areas such as power and telecommunications. Moreover, the International Y2K Cooperation Center's Global Status

Watch system reflects self-reported data and, as discussed earlier, concentrates on the reporting of problems that are not "normal" for a particular country.

REPORTED YEAR-2000 INCIDENTS ADDRESSED QUICKLY AND HAD LITTLE EFFECT ON THE DELIVERY OF KEY SERVICES

Few Year 2000-related errors reported during the rollover affected the delivery of key services because they were reported to be corrected quickly and/or contingency plans were implemented. A key reason that Year 2000-related errors had little effect on business operations and the delivery of key services is that federal agencies and other organizations used the rollover weekend to identify and correct errors before the problem resulted in operational consequences.

In guidance on planning for the rollover period, called "day one" or "day zero" planning,[11] we stated that organizations should activate coordination/command center(s), conduct facility inspections, and perform post-rollover tests, evaluations, and assessments of key business processes and supporting systems. According to the Chair of the President's Council, every emergency operating center in the federal government was operating on January 1, 2000, and agencies used the weekend to test their systems and operations. In addition, the Chair stated that organizations running critical services in the private sector were also staffed on January 1, 2000. For example, major banks and exchanges both in the United States and in foreign countries used the rollover weekend for final systems and interconnectivity testing in the year 2000 prior to opening for business.

[11] *GAO/AIMD-10.1.22, October 1999.*

The following are specific examples of how testing during the rollover weekend helped to identify and correct problems quickly.

- Shortly after the rollover to the year 2000, the General Services Administration and other agencies began checking federally owned and leased buildings to determine whether any Year 2000-related problems had occurred. As a result of these inspections, certain building operations—such as access control systems—were found to have malfunctioned and were corrected and/or contingency plans implemented.

- A "zero day" test of the DOE Oak Ridge facility's Dynamic Special Nuclear Material Control and Accountability System—a system normally not operating during the weekend—found a Year 2000-related file transfer error. After the rollover, one segment of the software began generating file identifiers with a 4-digit date format, while the file transfer software was expecting a 2-digit format. As a result, the test of the transfer failed. According to DOE, contingency plans that had been updated and tested because of the Year 2000 problem were implemented and magnetic tapes were used to successfully transfer the information and the Year 2000 failure was corrected a short time later.

- A foreign country reported to the International Y2K Cooperation Center's Global Status Watch system on January 2, 2000, that "numerous tests [were] carried out in banking, administration, and industries. Only minor problems [were found], corrected on the spot."

Reported Year 2000-Related Errors in the Federal Government

Before the rollover period, we testified before you that the federal government's overall progress had been significant—from a low of compliant mission-critical systems of 19 percent in August 1997 to a reported 99 percent in October 1999.[12] We also testified that while not all actions were completed at that time, the government had made progress in addressing our recommendations related to the key areas of priority-setting, end-to-end testing, and business continuity and contingency plans.

The federal government's efforts have paid off. During the rollover period, most Year 2000-related errors in the federal government were minor and did not have an effect on operations or the delivery of services. Even those that were significant (those that resulted in degraded service or, if not corrected, would have resulted in degraded service) were mitigated by quick action to fix the problem or through the implementation of contingency plans. Among the most significant incidents were the following.

- On January 1, 2000, the Deputy Secretary of Defense reported that one of its satellite-based intelligence systems experienced a Year 2000 failure shortly after the rollover of Greenwich Mean Time; Defense was not able to process information from that system. According to the Deputy Secretary, the problem was with the ground processing station, not the satellite itself. The Deputy Secretary also stated that Defense adopted backup procedures, which resulted in its operating at less than its full peacetime level of activity but allowed it to continue to meet

[12]*GAO/T-AIMD-00-37, November 4, 1999.*

its high-priority needs. Defense reported that the satellite ground processing system was returned to full operational status on January 3, 2000.

- The Health Care Financing Administration's (HCFA) Medicare program, a high-impact program, was affected by Year 2000-related errors experienced by its business partners. For example, on January 3, HCFA was informed that a bank that handles electronic fund transfer transactions for six contractors to the Federal Reserve could not receive those transactions electronically. HCFA developed a temporary workaround—having the contractors send diskettes with the transactions to the bank via overnight mail until the bank fixed and tested the electronic communication software error on January 6, 2000. While this workaround allowed HCFA to make payments to providers within the legislatively required 30 days, payments were nevertheless delayed. Specifically, $52.8 million in payments to Medicare Part A health care providers (e.g., hospitals and nursing facilities) was delayed 2 days, and $135.5 million in payments was delayed 1 day.

  Medicare payments to providers have also being delayed because claims have been submitted dated 1900 or 2099, leading to the claims being returned. Five Medicare data centers reported that they received about 26,000 claims from providers with these erroneous dates in the first week of the new year. Most of these claims were traced to providers that had not upgraded their systems. The Medicare contractors have advised the providers to update their systems, and HCFA has instructed the data centers to return claims with erroneous dates.[13]

[13]Before receiving this instruction from HCFA, one contractor had electronically modified about 11,000 claims with erroneous dates. According to HCFA's Deputy Director of Information Services, HCFA directed this contractor to stop this practice because it was concerned about modifying claims information without the concurrence of the provider.

- The Federal Aviation Administration's (FAA) air traffic control system, another high-impact program, reported experiencing Y2K-related systems problems. According to FAA, none affected safety, service, or capacity and some merely involved inaccurate date displays. In all cases, FAA reported that it was able to quickly fix the system or implement contingency plans that allowed operations to continue.

Two key FAA systems with problems that impaired operations were the Low Level Wind Shear Alert System and a contractor-maintained Kavouras Graphic Weather Display System. In the case of the Low Level Wind Shear Alert System, the system displayed an error at eight sites[14] following the rollover from 1999 to 2000 Greenwich Mean Time, and failed to operate. FAA field staff rebooted the systems, and the longest length of time that one of the systems took to return to normal operations was 2 hours and 12 minutes.[15] Because the systems were not operational for this short period of time and because FAA does not operate backup systems, this problem could have affected aviation operations if weather conditions had been severe. In the case of the Kavouras Graphic Weather Display System, ten minutes after the Greenwich Mean Time rollover, the system began sending data showing the year as 2010. This resulted in the system's rejecting weather data from the National Weather Service and failing to properly update data going to 13 Automated Flight Service Stations.[16] Within 10 minutes, the contractor reloaded system software in order to restore the service

[14] Tampa FL, Denver CO, Atlanta GA, Orlando FL, Chicago IL, St. Louis MO, LaGuardia NY, and New Orleans LA.
[15] The length of time these systems were out of operation varied widely, ranging from 3 minutes at one site to 2 hours and 12 minutes at another site.
[16] Altoona PA, Leesburg VA, Millville NJ, Macon GA, Loiusville KY, Columbia MO, Conroe TX, Elkins WV, Buffalo NY, Williamsport PA, McKeller TN, Gainsville FL, and Wichita KS.

and all systems were reported to be normal in about 2 hours.

Reported Year 2000-Related Errors in State and Local Government

As we previously testified,[17] the Departments of Agriculture, Health and Human Services, and Labor took action to help states successfully transition the 10 high-impact state-administered federal programs into the year 2000.[18] For example, the Department of Agriculture's Food and Nutrition Service obtained a contractor to conduct on-site visits to certain states and territories to provide technical assistance in areas such as software testing and contingency planning. The success of these efforts is demonstrated by the relatively minor Year 2000-related errors reported in these programs. In total, the Departments of Agriculture, Health and Human Services, and Labor reported that 11 states and territories had Year 2000 errors in one or more state-administered federal programs. These errors ranged from cosmetic printing or display problems to failures that resulted in minor disruptions of services. For example:

- Oregon had Year 2000-related errors in systems used for the Food Stamps, Child Support Enforcement, and Temporary Assistance for Needy Families programs. Regarding food stamps, the state's system for processing daily updates failed, creating a backlog of batch records. This problem was corrected by the installation of a new system on the next business

[17] *Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs* (GAO/T-AIMD-00-9, October 6, 1999), *Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits* (GAO/T-AIMD-99-241 July 15, 1999), and *Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance* (GAO/T-AIMD/GGD-99-221, June 23, 1999).

[18] The 10 high-impact state-administered federal programs are the Department of Agriculture's Child Nutrition, Food Stamps, and Special Supplemental Nutrition Program for Women, Infants, and Children; the Department of Health and Human Services' Child Care, Child Support Enforcement, Child Welfare, Low Income Home Energy Assistance Program, Medicaid, and Temporary Assistance for Needy Families; and the Department of Labor's Unemployment Insurance.

day, and no impact on business operations was reported. The state's system that tracks data in numerous programs, including Child Support Enforcement and Temporary Assistance for Needy Families, had a Year 2000-related problem that was fixed by January 7, 2000. This problem resulted in a 1-day delay in payments to clients.

- Florida and Kentucky reported Year 2000-related problems with their unemployment benefits' automated telephone call processing system which would not allow claims to be processed for claimants filing claims on January 3, 2000, who had earnings in 1999. About 100 claimants were affected in Florida and fewer than 50 in Kentucky. Claimants were instructed to complete and mail claims forms that had already been provided in advance. Florida reported correcting its system on January 4, while Kentucky reported fixing the problem on January 7.

- Guam reported it had successfully implemented contingency plans (i.e., manual processing) in the Food Stamps, Women, Infants, and Children, Medicaid, Temporary Assistance for Needy Families, Child Care, and Child Welfare programs. Such contingencies were necessary because the systems that supported these programs were not compliant and the replacement systems were not implemented before the century change.

In addition to state-administered federal human services programs, other state and local Year 2000-related errors were found. Examples include Year 2000-related problems with issuing drivers licenses for the wrong number of years and marriage license software registering the date as 1900 (both of these problems were reported as corrected). In another example, the Navajo

Nation Law Enforcement Office reported that seven of its eight computer-aided dispatch system servers failed and a manual process was used until the servers were fixed. According to a Navajo Nation Law Enforcement Office information systems analyst, all of the servers were fixed by January 19, 2000.

Reported Infrastructure and Key Sector Year 2000-Related Errors

Essential to the nation's transition to the year 2000 was the successful rollover of the organizations that manage the United State's infrastructure (i.e., energy, telecommunications, and water) and major sectors (e.g., banking and finance). Fortunately, there were no reported Year 2000-related errors in these sectors during the rollover period that affected their ability to continue providing these critical services. The leadership of the President's Council on Year 2000 Conversion and federal agencies which oversaw or created partnerships with major private-sector entities were essential to this success.

Many of the reported problems in the private sector related to the retail sector, including a retailer whose cash registers and other systems did not work until a software patch was installed, slot machines that did not work, and a small business that could not access its accounting information. Perhaps the most widespread Year 2000-related problem related to retail credit card processing. Credit card companies reported to financial regulators on January 6, 2000, that they had identified a Year 2000 failure resulting in over 470,000 duplicate transations on charges generated after January 1, 2000. The problem was due to over 7,000 small businesses using a particular electronic credit card processing system that they had not upgraded although the

vendor had made the patch available since March 1999. The merchants were notified of the problem and the credit card companies prohibited them from settlement services until their systems had been upgraded.

According to an official at the Federal Reserve, credit card industry representatives participating in an industry-wide effort to resolve this issue reported that as of January 19, 2000, a small number of merchants have been contacted, and over 5,800 merchants have fixed their systems. According to industry officials, because the credit card companies identified the duplicate transactions and reconciled the appropriate accounts with the affected merchants before items were posted to cardholder accounts, the duplications will probably not show up on customer billing statements.

Another Year 2000 incident occurred in the Federal Reserve System, which is instrumental to our nation's economic well-being since it provides depository institutions and government agencies with services such as transferring funds and securities. On January 3, 2000, the Federal Reserve Bank of Chicago reported a Year 2000 failure involving the transmission of about $700,000 in tax payments of 68 area banks to the Treasury's general account. Banks have various options for providing payment instructions to make tax payments to the Treasury using a voice response mechanism. However, an interface linking the Federal Reserve Bank of Chicago voice response unit with the Treasury, Tax and Loan system did not operate properly during the rollover period and it was unable to transfer tax payments totaling nearly $700,000 to the Treasury for banks that had used the voice response system (the Chicago Reserve processed about $5 billion in tax payments that day). The problem was corrected overnight and the tax

payments were processed the next day on January 3.

Reported International Year 2000-Related Errors

The President's Council on Year 2000 Conversion launched several initiatives in the international arena to address Year 2000 readiness in foreign countries. In particular, the Chair of the President's Council attended National Y2K Coordinators' meetings hosted by the United Nations and is a member of the Steering Committee of the International Y2K Cooperation Center. Further, as we testified on October 21, through its leadership of the President's Council's International Relations Working Group, the Department of State had worked to increase awareness of the Year 2000 problem throughout the world, collected and shared information on the problem with other federal agencies and foreign nations, and encouraged the remediation of faulty computer systems.[19]

Several foreign countries reported Year 2000-related errors to the International Y2K Cooperation Center's Global Status Watch system, but none were reported to have resulted in reduced capacity, capability, or service. For example:

- On January 5, 2000 Grenada reported that a compliant version of the computer systems for their customs services would not be installed until January 30, but that a manual backup system was "just as efficient."
- On January 6, 2000, Kazakhstan reported that a technology process at a power station had been handled manually since January 1, 2000, because noncompliant systems had not been

[19] *Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning* (GAO/T-AIMD-00-25, October 25, 1999).

replaced due to a lack of funds. According to the report, "manual handling causes certain difficulties, since at every power unit there are 250 devices to be controlled."

- On January 12, 2000, the Sudan reported that the interbank communications between two banks was delayed by 2 days due to a Year 2000 problem in the communications software. This problem was reported as fixed.

Other Year 2000-related errors were also found. For example, in England before the change of century, retailers had problems with credit card readers that looked 4-days ahead. According to England's government millennium center, this problem affected about 5 percent of terminals supplied by banks to process credit and debit card transactions. The problem was reported to have been largely resolved by the morning of December 30.

A variety of biomedical devices had Year 2000-related errors in foreign countries but none were reported to affect patient safety. For example, Sri Lanka reported that a hospital found that two blood gas analyzers were noncompliant. However, Sri Lanka reported that the problem had no significant effect on the clinical tests being carried out by the analyzers. Another hospital in Sri Lanka found that a E.C.G. Monitoring Unit was not compliant and that it could not be used.

LESSONS LEARNED FROM THE GOVERNMENT'S YEAR 2000 EFFORTS CAN BE USED TO IMPROVE MANAGEMENT OF INFORMATION TECHNOLOGY

For many federal agencies, the threat posed by the Year 2000 problem was a much-needed wake-up call. Because of the urgency of the issue, agencies could not afford to carry on in the same manner that had resulted in over a decade of poor information technology planning and program

management. As we reported in October 1999, the Year 2000 problem has laid a foundation for longer term improvements in the way the federal government views, manages, and protects computer systems supporting the nation's critical infrastructure.[20] Among the lessons learned were the importance of

- providing high-level congressional and executive branch leadership,
- understanding the importance of computer-supported operations,
- providing standard guidance,
- establishing partnerships,
- facilitating progress and monitoring performance, and
- implementing fundamental information technology improvements.

A recent report issued jointly by the Intergovernmental Advisory Board[21] and the General Services Administration provides information on similar experiences from federal agencies, states, local governments, and foreign countries.[22]

Providing High-level Congressional and Executive Branch Leadership

One of the most important factors in prompting attention and action on the Year 2000 problem has been proactive leadership at the highest levels of government. In particular, congressional

[20] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).
[21] The Intergovernmental Advisory Board was established to bridge the gap between federal, state, and local governments and to educate information technology professionals nationwide on finding solutions to intergovernmental challenges.
[22] *The Many Silver Linings Of The Year 2000 Challenges* (Intergovernmental Advisory Board in cooperation with the General Services Administration, January 2000).

oversight played a central role in addressing the Year 2000 challenge. For example, congressional hearings on agency-specific, national, governmentwide, and international Year 2000 problems exposed the threat that this problem posed to the public. In addition, the President's Council on Year 2000 Conversion provided strong, effective day-to-day leadership, focusing attention on the problem and providing a forum for high-level communication and partnerships among leaders in the government, the private sector, and the international community.

In the *Silver Linings* report, Georgia reported similar experiences with the effectiveness of executive branch leadership and legislative oversight. Georgia's Chief Information Officer reported that the principal direction for the state's Year 2000 program was set by the governor. Further, Georgia created a Y2K Executive Oversight Committee comprised of members of the state legislature and representatives from the state's executive branch that provided oversight and support.

Understanding the Importance of Computer-supported Operations

According to officials involved in conversion efforts, the Year 2000 challenge served as notice to many who were previously unaware of our nation's extensive dependence on computers. For example, the Secretary of Transportation stated that the Year 2000 issue had caused the department to become more enlightened about the importance of technology in its ability to deliver services, and that prior to the Year 2000 issue, he did not fully recognize the degree to which technology was being used in the transportation sector.

The *Silver Linings* report also highlighted benefits in this area. For example, Michigan reported that it had to focus on its core business processes and how they work, which it believes will be useful in identifying opportunities for information technology to play a pivotal role in transforming business practices. The Commonwealth of Virginia reported that one area it can capitalize on to improve its use and management of information technology is the extent to which such technology has permeated agency operations, and the attendant operational risks such dependencies entail.

In addition, the telecommunications sector stated that due to the Year 2000 problem, management now fully understands its dependence on technology and the importance of good engineering practice, process, and continuity. Similarly, the pharmaceutical industry reported that that it had spent a great deal of resources understanding every aspect of its downstream distribution system.

Providing Standard Guidance

Standard guidance that was universally accepted, adopted, and implemented facilitated Year 2000 conversion efforts and related oversight. In particular, guidance issued by OMB, the Chief Information Officers Council, and by us (1) provided a level of consistency across government by providing standard terms, tools, and techniques based on best practices, (2) imposed structure and discipline, (3) increased the rigor of testing and assessment efforts, (4) promoted consistency in data gathering and reporting, and (5) facilitated evaluation of actions by both agency

management and auditors. In the *Silver Linings* report, Michigan noted that it developed a consistent methodology for managing large information technology projects that it can carry forward.

Establishing Partnerships

To address the Year 2000 problem from a national perspective, the President's Council on Year 2000 Conversion and federal agencies established partnerships with several private-sector organizations, such as the North American Electric Reliability Council, to gather information critical to the nation's Year 2000 efforts and to address issues such as contingency planning. The Department of Energy reported that this private/public partnership was a benefit of the Year 2000 problem.

Other types of partnerships were also formed to address the Year 2000 issue, partnerships that should serve the nation well in the future. Several organizations reported to the President's Council on Year 2000 Conversion on the benefits of such partnerships. For example,

- The telecommunications industry reported that industries came together to support a common national interest.
- The oil industry reported that U.S. oil companies formed informal partnerships with associations in other countries.

In the *Silver Linings* report, Tennessee reported that the Year 2000 challenge encouraged all parties, especially in the government arena, to work together.

Facilitating Progress and Monitoring Performance

Both the executive branch and the Congress used techniques to facilitate and monitor performance in addressing Year 2000 conversion activities. During 1997, OMB instituted a quarterly reporting routine to facilitate monitoring of agency progress in making their critical systems compliant. In addition, many congressional committees actively monitored progress by holding hearings to obtain information on the Year 2000 readiness of federal agencies, states, localities, and other important nonfederal entities, such as the securities industry.

The development of project metrics to monitor progress internal to the organization was also a useful tool that was often developed in response to the Year 2000 challenge. In the *Silver Linings* report, agencies and states cited the following.

- The Department of Housing and Urban Development reported that it developed a tracking system to track progress and view interdependent relationships between information development efforts.
- The U.S. Customs Service reported that it developed a master schedule that was the foundation for measuring project progress.
- Michigan reported that it determined the need to develop a comprehensive project reporting system.
- North Carolina reported that statewide project planning and analysis as well as statewide project management and status reporting were Year 2000 activities that set the groundwork for a new, more efficient direction in enterprise management and business integration.

Implementing Fundamental Information Technology Improvements

The Year 2000 challenge resulted in many agencies' taking charge of their information technology resources in much more active ways than they have in the past, and provided them with the incentive and opportunity to assume control of their information technology environment. In many instances, it forced agencies to inventory their information systems, link those systems to agency core business processes, and jettison systems of marginal value. Also, agencies focused on their relationships with business partners critical to the delivery of services, especially for the government's 43 high impact programs. Moreover, agencies' development of business continuity and contingency plans should also help in the future in the event that an emergency occurs that negatively effects an agency's ability to perform services electronically.

The Year 2000 problem has also prompted some agencies to establish much-needed information technology policies in areas such as configuration management, risk management, and software testing. In addition, Year 2000 efforts have reinforced an understanding of the importance of consistent and persistent top management attention, which is essential to solving any intractable problem. According to officials at OMB, the Year 2000 problem also gave agency Chief Information Officers a "crash course" in how to accomplish projects. Many Chief Information Officers were relatively new in their positions and expediting Year 2000 efforts required many of them to quickly gain an understanding of their agency's systems, work extensively with agency program managers and Chief Financial Officers, and become familiar with budgeting and financial management practices.

Many of these same critical information management technology practices were also cited as improvements in the *Silver Linings* report. For example, (1) Georgia reported that new testing standards were initiated to meet critical Year 2000 deadlines, (2) Michigan reported that lessons learned for the future included the development of a formal risk analysis and comprehensive quality assurance program, and (3) Howard County, Maryland, reported that its Year 2000 projects required a complete inventory and assessment of technology resources used throughout county government.

- - - - -

While the end of the Year 2000 challenge is in sight, it is crucial that organizations not lose the momentum that they have established in conquering this issue. These organizations must remain vigilant in identifying and reporting Year 2000-related incidents, especially during the end of February. Moreover, it is important that the government and individual organizations institutionalize the processes that they have established to contend with the Year 2000 problem so that future information technology initiatives can benefit from this undertaking and the valuable long-term lessons it has spawned.

Mr. Chairman, Ms. Chairwoman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the Subcommittees may have at this time.

Contacts

For information about this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssenj.aimd@gao.gov.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of our review were to assess and report on (1) the response of the ICC and key federal agencies during the century rollover period, and (2) the nature and extent of Y2K-induced disruptions that occurred during the rollover period. In addition, as requested, we reported on lessons learned by the government and others while correcting their Year 2000 problems.

To meet these objectives, we placed observers at the ICC, 13 key federal organizations (see table 4), the 10 FEMA Regional Operations Centers, and the District of Columbia during the rollover weekend.

Table 4: Federal Organizations Where GAO Observed Rollover Activity

Federal Organization
Information Coordination Center
FEMA
Federal Aviation Administration
Social Security Administration
Department of Education
Department of Veterans Affairs
Department of Health and Human Services
HCFA
Food and Drug Administration
Federal Communications Commission
Federal Reserve System
Department of State
Department of Defense
U.S. Postal Service

As part of observing the rollover, we obtained and reviewed agency day one strategies, reviewed ICRS and incident reports, and discussed issues with appropriate personnel, including the Director of the ICC. We also reviewed key ICC documentation, such as the ICC Operations Guide.

We performed our work between November 1999 and mid-January 2000 in Washington D.C., Baltimore, MD, Herndon, VA, Rockville, MD, Piscataway, NJ, Maynard, MA, Philadelphia, PA, Atlanta, GA, Chicago, IL, Denton, TX, San Francisco, CA, Kansas City, MO, Bothell, WA, Denver, CO, and Martinsburg, WV. Our work was performed in accordance with generally accepted government auditing standards.

(511817)

Mr. HORN. It is always a pleasure to have the Commissioner of Internal Revenue here. We will see you again on April 15th. We would love to hear your statement, because you had a lot of burdens counting on it, people that wanted refunds and all the rest of it. So thank you, Commissioner, for being here.

Mr. ROSSOTTI. Thank you, Mr. Chairman. It is good to be here. Madam Chairman and distinguished Members, I am very pleased to report that the IRS experienced a smooth Y2K rollover starting on December 29th and continuing up to the present with fewer problems this January than we normally experience in a normal January. To date, we have had good success. It was hard work and our success can be attributed to the comprehensive planning and preparations we have conducted over the last 3½ years. We also are very grateful for the guidance and assistance you provided, your committee, as well as Mr. Koskinen and GAO.

I do want to note we cannot yet declare total victory on Y2K at the IRS. Some risks do remain, and in particular, we have to be very vigilant about Y2K problems that could still crop up during our high volume tax filing season, which really starts in February and continues through April.

As I discussed in previous hearings, the scope of the Y2K problem at the IRS was enormous and required a significant investment, about $1.3 billion, to plan and prepare.

But fortunately, that investment was made. Had we not adequately prepared for Y2K, I think it is fair to say the tax system of the United States would simply have ground to a halt. In my written testimony, I described several scenarios for today, I picked out a few of the events that would have occurred.

For example, our 14-year-old system for entering data from paper tax returns would have stopped working if we had simply allowed it to roll over without modification. This particular combination of hardware, software and third-party products could not be renovated, and therefore, was totally redesigned and replaced during 1998 and 1999. Without this system, about 90 million individual income tax returns that come in on paper would have just been piling up right now.

Second, interest and penalty calculations would have been incorrect and would have generated wrong notices to taxpayers. For example, if we had not replaced the system, we would have sent about 67 million wrong notices to taxpayers telling them that they owe money to the IRS. Those numbers would have been wrong.

Third, our data transfers with important external organizations such as the financial management service and the Federal Reserve Bank would have failed because of incompatible dates. This would have impaired or eliminated the ability to issue about 80 million refunds.

Just a final example, I think this is particularly interesting, and certainly not unexpected, but after years of fixing and testing these systems, we did one final end-to-end test that was completed about the middle of December. This particular final end-to-end test identified 175 problems. Some of those would have been very serious had we not fixed them at the end. For example, a system that generates new balance notices to taxpayers for certain tax periods was

displaying the date as 2099 instead of 1999 for some of those notices.

So if this problem had not been fixed, we would have been sending out hundreds of thousands of notices to taxpayers with incorrect tax periods and wrong payment dates that would have generated mass confusion among those taxpayers, and this was just only one example. There are many more scenarios in my written testimony. Of course, none of these things actually did happen, and that was simply because we acted in time to solve the problems.

Now, the question is sometimes asked in the form of was Y2K a blessing in disguise? I would have to say that I would not consider it to have been a blessing, whether it was disguised or not disguised, but there are some important residual benefits in the IRS that we will realize from the investment. I will mention the four most important.

The first is we did replace a lot of obsolete hardware and system software products. As a result of the Y2K program, most of our hardware in the IRS has been replaced, since most of it was really obsolete, and software releases have been brought up-to-date. This bringing up-to-date of this infrastructure is essential for supporting what we are now embarked on, our technology modernization program, and, of course, it is imperative that we have adequate annual replacements of hardware and regular routine upgrades of software releases in order to keep this vast installed base up-to-date.

Second, we did implement some very important improvements in our program management practices. Our Y2K program was successful largely because effective program management practices were implemented over the last 3 years. These practices will be extremely valuable as we now move forward with our technology modernization program.

I do want to note as challenging as Y2K was, our modernization program imposes even more and different challenges because it involves major business changes as well as technology.

Third, we were able to standardize many products. The IRS-installed base of hardware and software was not only obsolete, it was heterogeneous in the extreme. The Y2K program has allowed us to set up and largely implement standard products. Because of our reorganization under the leadership of our CIO, Paul Cosgrave, we now have the management structure and delegated authority in place to make design and procurement decisions to maintain standardization of technology.

Finally, we implemented improved inventory management. GAO has justly criticized the IRS for years for the poor condition of our IT inventory. Because of Y2K, we were forced to examine our inventory and bring it up-to-date as never before. So the condition of our inventory records is greatly improved, although I have to note it is still not fully where it needs to be, and there is much that needs to be done in the future on that problem.

In conclusion, Mr. Chairman, we are gratified with our results. I stress there are still some risks that remain. Clearly, we gained some residual benefits which will be of great value as we proceed to our even more challenging business system modernization programs. These benefits will only be realized if we actively continue

the practices established during Y2K, including regular replacement and upgrades of hardware and software. We will keep the subcommittees apprised of any remaining problems and our actions to correct them.

I thank you for the opportunity to discuss our efforts, and certainly thank you for your interest and support over the last 3 years.

Mr. HORN. Well, we thank you very much.

[The prepared statement of Mr. Rossotti follows:]

TESTIMONY OF
COMMISSIONER OF INTERNAL REVENUE
CHARLES O. ROSSOTTI
JOINT HEARING BEFORE THE
HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
AND HOUSE COMMITTEE OF SCIENCE
SUBCOMMITTEE ON TECHNOLOGY
ON
Y2K CONVERSION RESULTS
JANUARY 27, 2000

INTRODUCTION

Mr. Chairman, Madam Chairman and distinguished Members of the Subcommittees, I welcome the opportunity to testify on the results of the IRS' Y2K conversion efforts. I am pleased to report that we experienced a smooth Y2K "roll-over weekend" between December 29 and January 3 with fewer glitches than we experience in a normal year. Our success to date was hard won and can be directly attributed to our comprehensive planning and preparations over the past three and a half years. We are also most grateful for the guidance and assistance you provided throughout this effort.

However, we cannot yet declare total victory on Y2K. Some risks remain and we must remain vigilant to Y2K problems beyond January 1, 2000. We must safeguard against problems during the high-volume tax-filing season from February through April – the most crucial period for Y2K issues at the IRS.

Today, I will discuss the scope of Y2K at the IRS, summarize the preparations undertaken to prepare for the new millennium, provide some examples of what could have gone wrong had we not fully prepared for Y2K, and finally, discuss some of the long-term benefits realized from our Y2K efforts.

PROGRAM SCOPE

IRS operations are critical to our nation. Each year the IRS collects over $1.7 trillion in tax revenue to support the operations of the Federal Government. The IRS also touches the lives of virtually all Americans.

In order to fulfill its mission, the IRS totally depends on its computer-based systems to process tax returns, issue refunds, credit payments, respond to more than 170 million taxpayer inquiries a year through our toll-free, 24-hours a day, 7-days a week telephone system, collect overdue taxes and audit 1.1 million returns. Due to the sheer size and complexity of its mission, it would be impossible for the IRS to rely on any type

of backup system or manual methods for more than very limited parts of our organization.

As I discussed in previous hearings, the scope of the Y2K challenge at the IRS was enormous. The IRS employs more than 100,000 individuals in over 700 locations across the United States. Making the IRS' Y2K problem even more challenging is the sheer number of affected information technology systems.

There were approximately 800,000 information technology (IT) items in our inventory that were assessed for compliance; renovated, replaced or retired; tested; and placed back into production. The technology ranged from custom applications programs to mainframe computers to commercial software products as well as thousands of non-IT items found in elevators and office equipment.

Without the significant investment in resources to plan and prepare for Y2K, there was a tremendous potential for significant disruptions to ongoing IRS operations. Fortunately, that investment was made. By comparison, our expenditure of $1.3 billion was significantly larger than that of the largest private financial institution which reported $950 million in expenditures.

PREPARATIONS FOR Y2K

To manage Y2K preparations, the IRS created the Century Date Change Project Office in 1997. Its two overriding goals were: (1) ensure the nation's tax processing systems function in the year 2000 and beyond; and (2) continue providing effective customer service to taxpayers while preparing for Y2K.

In late 1997, an executive steering committee, which I chaired, was established to oversee the whole process. The committee met at least monthly from November 1997 through January 2000. All risks and action items identified in discussions were rigorously tracked.

The past three and a half years of Y2K readiness activities focused on the following major tasks:

- Software code conversion,
- Commercial hardware and software product compliance,
- End-to-End testing,
- Independent Verification and Validation, and
- Roll-Over weekend execution.

Software Code Conversion

The IRS maintains over 90,000 custom applications programs, and over 51 million lines of code to support our tax processing and administrative support operations.

Each line of code was assessed, appropriate renovations made, and tested according to a well-defined, 14- step conversion process.

The process directly followed the General Accounting Office's (GAO) Year 2000 Conversion Model and includes three levels of testing: developer testing, independent system acceptability testing, and finally, End-to-End testing. While most of our software was converted and implemented by January 1999, changes that were made to the Tax Code for the filing season required these programs to be re-tested for compliance, further complicating the task.

Commercial Hardware and Software Compliance

Much of our infrastructure is antiquated and had to be upgraded or replaced to achieve Y2K compliance. This included many of our mainframe computers, which were either upgraded or replaced, and most of our minicomputers, many of which were retired or replaced with fewer systems running in consolidated locations. The rest were upgraded to Y2K compliant operating systems and database management systems. Capacity upgrades were required of many of these machines to support the new Y2K compliant versions of operating systems, database management systems, and customer software applications. Many of the older machines were also no longer supported by the manufacturers and were subject to breakdowns and processing failures.

Our network of personal computers and laptops was upgraded from a variety of equipment dating back over 20 years, including "dumb" terminals, and systems running with outdated processors. The organization also maintained over 4,000 different software products, including 11 e-mail systems. Most of this equipment was replaced across the entire IRS with new Pentium-class personal computers and laptops, running standard software.

The conversion of IRS hardware and commercial software products was also subject to the rigorous, 14-step conversion process. In addition to receiving Y2K compliance certification from the manufacturer of each item, the IRS tested each type of mainframe, minicomputer, personal computer, telecommunications device, and commercial software product in the inventory.

End-to-End Testing

Like many other private and public organizations, the IRS conducted integration tests to ensure that our Y2K systems would actually function *together* in the Year 2000. End-to-End testing began in July 1998 and was completed in December 1999. This testing environment included all of our converted software code, telecommunications devices, and commercial hardware and software products.

Since it was impossible to take our critical tax processing systems off-line for an extended period of time to conduct this testing, we built a replica of the January 2000 processing environment. This replica, or "test bed," included each type of hardware and

software device used by the IRS. All of the IRS' main tax processing systems were exercised on the test bed using Year 2000 dates. The final End-to-End test, which was conducted after other testing was completed, identified 175 errors that were corrected prior to January 1, 2000. We also completed external trading partner testing for over 1,400 data exchanges, and conducted independent Y2K readiness assessments of our 13 key external trading partners, such as the Social Security Administration.

Independent Verification and Validation

In addition to our quality assurance and End-to-End testing, we also conducted a series of independent verification and validation tests to address a series of concerns raised by the GAO and the Treasury Inspector General for Tax Administration in their reviews of our Year 2000 program.

- We contracted for a 100 percent review of our software code renovation. These reviews discovered an error rate of approximately .006 percent. As a result of this effort, 4,364 lines of code required reprogramming to correct confirmed errors.

- We also contracted for an independent review of our third party software products. This review assessed over 21,000 products, and identified almost 3,000 confirmed errors, which were corrected prior to January 1, 2000.

- We also conducted a series of Independent Assessment and Readiness Reviews of our Service Centers and District offices to ensure that their self-reported Year 2000 results were verified prior to the roll-over weekend. As a result of these visits, we identified 673 corrective actions that were taken to ensure compliance.

Roll-Over Weekend Execution

The IRS devoted significant resources to develop an "end game" strategy that guided our activities during the critical roll-over weekend of December 31, 1999, through January 3, 2000. During this weekend, over 11,000 specific tasks and checkpoints were planned, executed and tracked. Using industry best practices and GAO guidance, the IRS planned and implemented the following activities:

- Created the Year 2000 Command Center for monitoring and reporting on the status of the roll-over;

- Kept all systems idle through the transition from 1999 to 2000;

- Conducted validation checks of all computer systems, computers, phone systems, and non-IT items (e.g., elevators, security systems and heating/cooling) at over 500 Posts of Duty around the country; and

- Provided for ongoing monitoring of key events during the current filing season to ensure that any emerging problems are identified as early as possible.

I am happy to report that our critical tax processing and administrative support systems are fully operational and that no major Year 2000 related problems or outages have occurred to date.

WHAT COULD HAVE GONE WRONG

As previously stated, the smooth transition to Year 2000 can be directly attributed to our thorough planning and preparation. However, had we not adequately planned for Y2K, the tax system would have ground to a halt. Some of the scenarios that Could have occurred are the following:

- Testing of our 14-year old data entry system for processing paper tax returns revealed that had we allowed it to roll-over to the Year 2000 without any modifications, the system could have stopped working. The combination of hardware, software and third party products on this old equipment could not be renovated, and was totally redesigned and replaced in 1998 and 1999. Without this system approximately 75 percent of individual income tax returns could have just piled up.

- Interest and penalty routines could have made incorrect calculations and generated incorrect notices to taxpayers. Virtually every balance due notice could have been wrong.

- Payment due dates and receipt dates could have been erroneously computed – once again, generating incorrect notices to taxpayers.

- IRS employees' passwords could have erroneously expired, preventing them from logging onto the systems.

- Database routines that select records for archival or disposal based on date could have erroneously archived or deleted volumes of data.

- Data transfers with external organizations such as the Financial Management Service and the Federal Reserve Bank could have failed, impairing our ability to issue over 80 million refunds to taxpayers.

- Federal Tax Deposits could not have been processed in a timely manner, resulting in the loss of millions of dollars of interest for the government, and potential collection actions against taxpayers who had paid their taxes but whose accounts had not been properly updated.

- Tax returns could not have been processed in a timely manner, resulting in paying interest to the taxpayers for refund returns. Many taxpayers could have filed duplicate returns thinking they had been lost, and taxpayer calls asking about the status of their return or refund could have soared.

Even after years of fixing and testing, our final end-to-end test, which was completed in December of 1999 identified 175 problems. These included such items as:

• The system that generates notices to taxpayers, explaining calculations of interest and penalties, was issuing notices to taxpayers, even though a request had been entered to stop the notice from being issued. Correcting this problem ensured we did not send these incorrect notices to taxpayers.

• The system which generates balance due notices to taxpayers was displaying the tax period and payment due date as 2099, not 1999. If this problem had not been fixed, we could have sent hundreds of thousands of notices to taxpayers with incorrect tax periods and payment due dates.

• The system which is used to review outgoing notices was displaying dates incorrectly and inconsistently. Had this problem not been corrected, we would have spent numerous staff hours correcting these notices. If these notices were not properly corrected manually, they would have displayed incorrect dates when sent to taxpayers.

LONG-TERM BENEFITS

The question is sometimes asked, "Was Y2K a blessing in disguise?" This question is asked because the dire consequences of failure required the IRS, as many other organizations, to address issues of long-standing concern. While I could not say that I consider the Y2K problem to have been any kind of blessing, disguised or otherwise, there are several important long-term residual benefits of having solved this problem. They fall into four categories:

Replacement of Hardware and Systems Software Products

Prior to the start of the Y2K project, the IRS installed base of computers and general-purpose software products (such as operating systems, data bases and utility software) was in many cases obsolete in the extreme. Hardware, such as the basic data entry systems, dated back to the 1970s. Many computers in the hands of revenue agents were early 1990 vintage DOS machines and the operating software releases were in many cases so old that the vendors did not currently support them.

As a result of the Y2K program, most of this hardware has been replaced with current technology and the software releases have been brought up to date. This up-to-date base of hardware and software is absolutely critical to provide reliable, efficient current operations and also is a prerequisite for supporting our technology modernization program. It is simply not feasible to deploy modernized computer applications on operating software and hardware that is no longer supported by the technology industry.

In order to avoid slipping back into the unacceptable state in which the IRS found itself three years ago, it is imperative that we maintain this installed based by adequate annual replacements of hardware and regular routine upgrades of software releases.

Improved Program Management Practices

At the time I arrived at the IRS, the agency had been heavily criticized for its inability to properly manage large-scale technology modernization programs. The criticism included: lack of engagement by business operators; lack of an appropriate governance process; and lack of effective program management procedures and staffing. The Y2K problem created the need and the opportunity to address all of these issues in a situation in which meeting dates was obviously an absolute necessity. The Y2K program, a large one by any standard, has been successful, largely because effective program management practices were implemented and improved over the last three years.

This experience will be extremely valuable as we move forward now with our major technology modernization program. The management approach we are using today stresses: active engagement by the top business leaders; adherence to a system life cycle methodology; adherence to business and technology architectural standards; early identification and management of risk; constant evaluation of projects; alignment of resources against our highest priorities through planning, re-planning and review of business cases; and clear guidance that all key implementation events will be assessed in light of all information at the time, and if necessary, schedules and objectives will be adjusted to reflect reality.

While we have made great progress in program management, we must still recognize that the IRS faces what is probably the largest single business system modernization program underway in the country. While there are many similarities to the Y2K program, the modernization program imposes greater challenges because it involves major business changes as well as new technology. For this reason, we must be realistic that there are significant risks associated with this program and that our task is to manage these risks in an orderly and systematic way.

Standardization of Products

The IRS installed base of hardware and software was not only obsolete, it was also heterogeneous in the extreme. Focusing just on software, the IRS had over 1,100 different mainframe third party software products, over 1,300 different minicomputer third party software systems, and a total of almost eight thousand software products of various kinds. In e-mail systems alone, we had 11 different systems with no common directory. In large measure, this situation reflected the fragmented nature of Information Services management and organization in the IRS in which many different business operations conducted their own IS operations and often purchased hardware and software.

Through the leadership of our CIO, Paul Cosgrave, the IS organization throughout the IRS has been brought together under one management. The Y2K program has allowed us to set up and largely implement standard products. For example, today we have one e-mail system throughout the IRS, and we have reduced the number of desktop products from about four thousand to three hundred.

Because of our reorganization, we now have the management structure and delegated authority in place to make design and procurement decisions to maintain standardization of technology.

Improved Inventory Management

Y2K also gave us the opportunity to improve significantly the quality of our IT inventory. GAO criticized the IRS for the poor condition of its inventory, but because of Y2K, we were forced to examine our inventory as never before. We retired millions of lines of local code and implemented national standard applications. Several thousand obsolete computers were removed from use. Old equipment, non-standard software, and commercial software not under maintenance contracts were removed from production and disposed of. Inventory teams visited each of our major tax processing sites and validated the inventory at that location against the database. Finally, massive record updates to our database were executed, providing more accurate information, such as point of contact, make, model, and version data. The condition of our inventory is now greatly improved although much work remains to be done.

IRS PROVIDES PENALTY RELIEF FOR Y2K-RELATED PROBLEMS

There is also another side to the Y2K coin. The Internal Revenue Service took steps to provide penalty and interest relief to taxpayers and businesses who might be unable to comply with the tax laws because of Y2K problems beyond *their* control.

Following up on legislation enacted this year, the IRS is prepared to waive tax penalties and interest for taxpayers who encounter major Y2K problems despite taking appropriate steps to prepare for the century date change. Taking a common-sense approach will help most taxpayers adequately prepare for Y2K, but the IRS stands ready to help if some taxpayers and businesses encounter Y2K tax problems beyond their control.

The IRS can provide Y2K tax penalty and interest relief in cases where: (1) taxpayers make a reasonable effort to become Y2K compliant; (2) a Y2K failure significantly affects a taxpayer's ability to comply with the tax laws, such as inability to file on time or make tax payments or deposits on schedule; (3) the tax law violation was unavoidable due to a Y2K failure or as a result of Y2K-related efforts to prevent disruption of essential services; and (4) taxpayers alert the IRS about the problem.

Penalty relief means the IRS can abate or waive tax penalties, such as those for failure to file, failure to pay and failure to deposit. Even if Y2K problems occur, most individual filers should have sufficient time to file their individual returns by this year's tax deadline. To date, no taxpayer has applied for penalty relief for Y2K related problems.

CONCLUSION

Mr. Chairman and Madam Chairman, in conclusion, we are gratified with the results of our successful Y2K conversion program, although I again stress that some risk remains through the remainder of this filing season. The enormous amount of work accomplished by our employees over the past three and a half years is directly responsible for our success. Without their skill and dedication, the IRS would have been unable to continue to operate the tax system of the United States.

The IRS gained valuable residual benefits, which will be of great value as we now proceed to our even more challenging business systems modernization program. However, these benefits will only be realized if we actively continue the practices established during Y2K, including regular replacement and upgrades of hardware and software.

We will keep the subcommittees apprised of any Year 2000 related problems and our actions to correct them. I thank you again for the opportunity to discuss the IRS's Y2K efforts and your continued interest and support.

Mr. HORN. As Mr. Koskinen leaves the scene, there is no question in my mind the toughest job in the executive branch is the Commissioner of Internal Revenue. If anybody is going to turn that agency around, you are.

So, thank you.

The last witness on this panel is Mr. Fernando Burbano, the Chief Information Officer of the Department of State. We are glad to have you here.

Mr. BURBANO. Thank you, Mr. Chairman, Madam Chairwoman and distinguished members of both committees. Since my oral testimony is limited to 5 minutes, my written testimony includes more detail.

As chairman of the CIO Council Subcommittee on Critical Infrastructure Protection, I am pleased to have this opportunity to discuss how lessons learned, products and processes developed in support of Y2K, can be leveraged into our ongoing critical infrastructure security efforts and challenges facing Federal agencies in implementing security pleasures.

As well, in my role as CIO of the State Department, I would like to thank you for providing me this opportunity to talk about the results and continuing impacts of the Department's successful Y2K preparation efforts. The Department of State, along with rest of the Federal Government, showed just how powerful and effective we can be when we are singularly focused and committed to solving a problem and are provided the necessary resources to get the job done.

First, let me quickly address the cost of preparing for Y2K. The question is, did we spend too much? The answer is very simple: Absolutely not. We should be careful not to confuse the lack of catastrophic disruptions with unnecessary preparations by the Federal Government.

Now, moving on to the actual results of the Y2K rollover and its impacts to the global community. In general, there are few and only minor Y2K failures reported internationally, and none that impacted the safety of American citizens worldwide. I believe this global success is a direct result of the U.S. Government's international outreach and awareness campaign led by the Department of State, the Department of Defense and the President's Council on the Y2K Conversion, in coordination with the United Nations and World Bank.

Embassies representing the U.S. presence in over 160 countries around the world played a key role in monitoring and reporting events in their host countries and post facilities through a Y2K task force convened in State's operations center. Additionally, internal State Department systems fared exceptionally well throughout the rollover, experiencing no significant failures among our mission critical, critical and routine systems.

As you are well aware, many of the products and processes developed to address Y2K problems can be applied to future challenges and serve as the foundation for managing issues with cross-agency and public-private boundaries, including critical infrastructure protection. In fact, much of the work already done is a prerequisite for PDD 63, critical infrastructure protection, Clinger-Cohen, and other government performance results act initiatives.

Specifically, Y2K preparation forced government agencies to take a close look at its IT applications and produce a complete prioritized inventory. This is a critical first step to identifying and refining the mission essential infrastructure as required by PDD 63.

The Y2K effort produced program management methodologies which were applied across all government agencies and included executive and congressional oversight, Assistant Secretary level management and repeatable standardized measures and processes. This management structure can also be applied to critical infrastructure protection.

All elements of the Federal Government reviewed and developed contingency plans for critical business processes. The development of these contingency plans resulted in a greater understanding by senior policy managers of the dependency of business processes on IT systems. Additionally, these plans are durable beyond Y2K established a foundation for all future contingency operations planning.

For the Y2K rollover period, the government developed a robust global reporting structural which can be leveraged into a mechanism for monitoring threats against critical infrastructure elements. For example, within the Department of State, we have developed a web-based geographic information system to collect cyber-threat information from all overseas posts. This tool can serve as a pilot system for other agencies to collect and analyze cyber-threat data.

Finally, Y2K preparation efforts increased the level of interagency cooperation and coordination between the public and private sectors. The same working level teamwork will be required to effectively implement critical infrastructure protection plans.

There are two areas which I believe allow the Federal Government to successfully overcome widespread Y2K problems in the face of an unmovable tight deadline.

First, continued participation by key congressional oversight organizations provided Federal Y2K programs the authority needed to push agency resources to their limits.

Second, the ability of Federal Y2K programs to rapidly obtain and more importantly retain adequate separate supplemental funding, specifically designated for Y2K, allowed each agency to acquire the resources necessary to achieve the time sensitive objectives.

This ability of Federal agencies to have access to a congressionally managed yet continuous separate supplemental funding stream designated specifically for the Y2K effort allowed Federal CIOs and Y2K program managers the ability to acquire and retain qualified resources in the needed quantity.

Critical infrastructure protection requires the same approach. Involvement by Congress and other oversight organizations to raise the level of awareness and visibility throughout the Federal community and overseas CIP implementation in support of national security goals is vital, and this activity is already underway.

But just as important to me and my colleagues through our government is access to funding which allows each of us to begin developing and implementing our plans in accordance with PDD 63 and other critical infrastructure protection guidance and statutes.

One of the key obstacles preventing agencies from immediately pursuing CIP initiatives is the lack of current funding for these projects. Due to the Federal Government's budget cycle, forecasting the future work is done 2 years prior to the budget year. Therefore, as new requirements are levied, current agency budgets do not reflect changing priorities and requirements, such as the need for critical infrastructure protection implementation initiative. In light of this, there are numerous events that have prevented agencies from adequately addressing current CIP implementation requirements in their fiscal year 2000 and fiscal year 2001 budgets.

First, the unprecedented and unpredictable growth of Internet use and technologies over the last 2 years; second, the corresponding collateral growth of the cyber underworld during this same period; third, the extent to which our daily business relies on Internet-based systems and the fundamental shift of business tools to be used in a web-based environment; finally, expanding CIP requirements on Federal agencies, including the recent critical infrastructure plan released and its 10 programs, some of which require immediate implementation.

These are just some of the reasons why Federal agencies are poorly positioned to successfully implement critical infrastructure to address the challenge posed by the ever-growing cyber underworld, not to mention to be in compliance with executive guidance. Although we of the CIO council fully understand fiscal constraints, reallocation of such a fraction of the current surplus would be a solid investment for the protection of the Federal Government's critical infrastructure.

In closing, it is my belief and the belief of members of my subcommittee and CIO's across the Federal Government that in order for the national CIP initiatives to be fully successful, continued congressional support as well as the ability to get access to specific CIP and security-related funding is vital. I cannot emphasize that without congressional-backed support, including adequate funding, we on the subcommittee of the critical infrastructure committee believe that the government will significantly fall short of national critical infrastructure protection goals. Thank you.

Mr. HORN. We thank you very much for that statement.

[The prepared statement of Mr. Burbano follows:]

**WRITTEN TESTIMONY OF FERNANDO BURBANO,
STATE DEPARTMENT CIO AND
CIO COUNCIL CIP SUBCOMMITTEE CHAIR
JANUARY 27, 2000**

I am pleased to submit this prepared testimony to Chairman Horn, Chairwoman Morella, and the distinguished members of the Subcommittee on Government Management, Information, and Technology, and members of the Subcommittee on Technology. This testimony will provide the Subcommittees' members details on the aftermath of Y2K and the continuing impacts of the federal government's preparatory efforts from two perspectives.

First, in my role as Chairman of the CIO Council's Subcommittee on Critical Infrastructure Protection (CIP), this testimony explains how lessons learned from the federal government's successful approach to managing Y2K efforts could be applied to government-wide efforts to implement Critical Infrastructure Protection initiatives. Similarly, this report also describes how products and processes developed in support of Y2K can be leveraged into each agency's ongoing critical infrastructure security efforts. As well, in my role as Chief Information Officer of the Department of State, this document summarizes the results of the Y2K rollover at our embassies and consulates around the world and briefly highlights the outcomes from the Department of State's successful Year 2000 preparation efforts. Finally, this testimony begins by quickly addressing the issue of whether or not the cost of the federal government's Y2K preparations, from my perspective as CIO of the State Department, was worth it.

Was the Cost of Y2K Preparations Worth It?

There has been much discussion and speculation surrounding the costs of preparing for Y2K. The question being posed is, "Did the federal government spend too much preparing itself for the Y2K bug?" The answer is unequivocally "no." As responsible government managers, we should be careful not to confuse the lack of catastrophic disruptions with unnecessary preparations by the federal government. By focusing attention at the highest levels of government and establishing a separate, unimpeded structure to oversee the Y2K effort and distribute the necessary resources to agency Y2K programs, the federal government showed just how powerful and effective it can be in addressing a large scale, time sensitive problem with potentially disastrous impacts. The federal government has taken, and continues to take, criticism for projects which don't deliver successful outcomes, or experience significant cost and schedule overruns. Therefore, in the case of Y2K, we should not second guess our success.

Myself and my CIO colleagues across the federal government take very seriously our responsibilities to serve American citizens. We, along with our counterparts in industry, made prudent, professional decisions to request, allocate, and manage funds to ensure critical processes and technologies will continue through and beyond the Year 2000. Observers and critics must only look as far as the continuing reports of Y2K glitches throughout the world as evidence of

our prudent and efficient management of the Y2K problem. Just consider the numbers of failures and their potentially far-reaching impacts had we not acted responsibly in addressing the Y2K issue. In short, the federal government of the United States could simply not afford failures and subsequent vulnerabilities to its systems and our overall approach for focusing attention and quickly supplying resources effectively delivered desired results: an uninterrupted technology and business transition into the year 2000.

Y2K Results - Worldwide Snapshot

In general, there were few significant Y2K failures reported internationally, and none that immediately impacted the safety of American citizens worldwide. This global success can, in large part, be attributed to the United States government's international outreach and awareness campaign led by the Department of State, Department of Defense, and the President's Council on the Year 2000 Conversion, and in coordination with the United Nations and World Bank. Embassies representing the United States' presence in over 160 countries around the world played a key role in monitoring and reporting events in their host countries and post facilities to our Y2K Task Force convened in State's Operations Center. Thankfully, all sites maintained normal operations.

However, there were Y2K-related incidents and failures that occurred throughout the world, including the United States. The following list of confirmed failures is just a sampling of what could have happened had the problem not been addressed.

- ***Canada:*** Computer controls on prison cell doors in British Columbia failed.
- ***Kazakhstan:*** Ekibastuz Hydroelectric Power Station-2 has handled its technology processes manually since January 1, 2000, because of non-compliant computers.
- ***Spain:*** Y2K problems were experienced in control systems for two out of nine nuclear reactors.
- ***United States:*** The Federal Reserve Bank in Chicago reported a Y2K glitch in transferring about $700,000 in tax payments from customers of 60 financial institutions in the region.
- ***Zimbabwe:*** The City of Harare's financial system failed.

Y2K Results - Department of State

Internal State Department systems faired extremely well through the rollover experiencing no significant failures among any of our mission critical, critical, or routine systems. State did, like most organizations, experienced a small number of minor failures to some of its systems as a result of Y2K. However, our pre-positioned business resumption teams quickly diagnosed and fixed each of the problems within hours and well before January 3rd, the first business day of the year 2000, so that none of State's core business or operations were impacted.

As evidenced by the small number of total Y2K-related incidents experienced by the Department, it is clear that State's early focus on the Y2K problem and our hard work and dedicated effort to manage and execute this enormous task proved to be a successful combination in preparing State's technology assets for Y2K. In fact, State's Y2K Program and its overall progress was recognized as a model of excellence by the Government Computer News (GCN) in achieving outstanding results in preparing for Y2K.

Operationally, the Department of State had responsibility for collecting, analyzing, and reporting the status of worldwide events as they unfolded. Therefore, we used our embassies around the world as our eyes in the field to assess their local situations and report the status of their post and host country shortly after the rollover on January 1st. Although no serious events occurred during the millennium transition, our processes and technologies which were developed for this massive data collection and analysis effort worked flawlessly and we are currently working to determine where they can be leveraged to support our future operations.

Y2K Lessons Learned and Critical Infrastructure Protection Re-use

The Year 2000 problem presented the federal government with many new challenges which had to be overcome in order for the State Department, and other federal agencies, to be successful in addressing the Y2K problem.

Due to the unique nature of the Y2K problem, we were forced to quickly develop and implement new approaches, methods, and technologies for solving Y2K-induced problems. However, many of these products and processes developed to address Y2K problems can be applied to future challenges and serve as the foundation for managing large scale problems which cross all agencies and require separate focus at both the policy and agency level, including Critical Infrastructure Protection.

Specifically, the following Y2K lessons learned and legacy products and processes can be leveraged directly into Critical Infrastructure Protection planning, management, and execution:

- ***Separate Supplemental Funding***: Provided agencies with separate supplemental funding, in addition to their core funding, to support implementation of Y2K remediation and preparation efforts. The majority of CIOs across the federal government believe that without this separate supplemental funding structure, their Y2K Programs would have failed.
- ***Senior-level Sponsorship***: By-in and leadership from key leaders within the federal government and individual agencies placed the responsibility and accountability of project tasks, activities, and milestones at levels that could quickly effect change and acquire needed resources.
- ***Repeatable and Measurable Metrics:*** Repeatable and measurable project performance metrics at both the agency-level and federal-level allowed Y2K Project Managers the ability to assess current status and progress against federal milestones.
- ***IT Product Inventory:*** A detailed product inventory of each agency's mission essential systems and information technology was thoroughly documented, tested at a system

level, independently verified, and placed under strict enterprise-wide configuration control.

- ***Contingency Plan Development:*** Mission-based contingency plans of all mission essential business processes were developed and tested.
- ***Global Reporting:*** Global, real-time reporting of specific Y2K status of vital domestic and international concerns to central data coordination centers.
- ***Public/Private Cooperation:*** Increased the level of coordination and cooperation between government agencies and private industry.

As a result of developing the products and instituting the processes listed above, the government has seemingly accelerated the process of implementing Critical Infrastructure Protection programs. In fact, much of the work already done is a prerequisite for PDD-63, CIP, Clinger-Cohen Act of 1996, and Government Performance and Results Act (GPRA) initiatives. The following table (***Table 1***) summarizes our assessment of the reusability of the items listed above.

Reuse Item	PDD-63	CIP Initiatives	Clinger-Cohen	GPRA
Separate supplemental Funding	**F**	**F**	-	-
Senior-level sponsorship	**F**	**F**	**F**	**F**
Repeatable and measurable metrics	**F**	**F**	**F**	**P**
IT Product inventory	**M**	**M**	**F**	**P**
Contingency Plan Development	**F**	**F**	-	-
Global reporting	**M**	**M**	**P**	**P**
Public/Private Cooperation	**F**	**F**	**M**	**P**

Legend
F - Full: Reuse Item can be fully leveraged into the federal initiative
M - Most: With some minor modification, the Reuse Item can be leveraged into the initiative
P - Partial: Some aspects of the reuse Item can be leveraged into the federal initiative

Table 1. Lessons Learned Reuse Assessment

Separate supplemental funding is needed to ensure resources are in place to support requirements which were unable to be included as part of our current budget cycle

I cannot emphasize enough how vital the separate supplemental funding stream was to our Y2K efforts. Without a separate supplemental funding source, I fully believe that State, and probably most federal agencies, would have failed.

Senior-level sponsorship is necessary for any large scale program to quickly effect change and acquire resources

Accountability and involvement by senior agency officials, including agency Secretaries, Under Secretaries, and Assistant Secretaries proved key to the success of Y2K programs. Due to the

high level of visibility within each agency, emphasis on the importance of addressing the Y2K problem trickled down through the organization and provided Y2K programs with adequate with remediation teams. Also, given the senior level involvement and responsibility, changes were quickly made and resources were made available when required by Y2K Program Managers to meet agency and government-wide milestones and goals.

Successful program management techniques, including metrics tracking and analysis, can be leveraged to support CIP/security initiatives

The Y2K effort required agencies to develop and implement effective program management methodologies to manage such a large scale, time sensitive task. These government-wide management approaches included Executive and Congressional oversight and agency-level performance measurement across a variety of areas, including project cost, technical issues, risk management, and schedule. This same management structure and discipline, including Assistant Secretary level management and repeatable standardized measures and processes, can also be applied to Critical Infrastructure Protection.

Detailed information technology inventories are the cornerstone of many federal security initiatives

Most agency Y2K preparations began with developing a complete, prioritized list of the organization's IT applications. This IT inventory is a critical first step to identifying and refining the Mission Essential Infrastructure of an agency as required by PDD-63.

Contingency Planning Efforts can be leveraged to support other federal initiatives

All elements of the federal government reviewed and developed contingency plans for critical business processes. The development of these contingency plans resulted in a greater understanding by senior policy managers of the dependency of business processes on IT systems. Additionally, these plans are durable beyond Y2K and establish the foundation for all future contingency operations planning.

Within the State Department, contingency planning focused on the need to maintain overall continuity of the Department of State's business, the pursuit of foreign policy in support of the United States strategic goals and national interests, in the face of potential Year 2000 failures.

In addition to the "Main State" Washington, DC headquarters in Foggy Bottom, the Department has 50 annexes in the local area, 16 passport agencies and 21 diplomatic security offices across the United States, 3 financial processing centers (Charleston, Paris and Bangkok) and posts and consulates around the world. Each of these has developed site and situation-specific contingency plans.

- ***Main State and Annexes***: Contingency plans for Main State and annexes have been prepared. Extensive event management planning includes provisions for key employees to be on site with all necessary work resources and personal effects.
- ***Regional Bureaus***: The Department's eight regional bureaus manage U.S. foreign policy in geographically defined areas (Europe, Africa, Western Hemisphere, etc.). Contingency plans have been formulated to cover bureau internal business processes as well as regional/post planning.
- ***Overseas Posts***: All embassies and consulates have developed contingency plans which address, at a minimum, the safety and security of staff and dependents, the physical integrity of post facilities and the continuity of core mission functions, including American citizen services.
- ***Passport Agencies:*** The Department's 16 passport agencies, including the National Passport Center, coordinate all operations through the Bureau of Consular Affairs (CA) which determines the distribution of workloads. Due to this strong central management, if there are failures whether internally to our systems or externally at these locations, guidance and response will be coordinated with CA. In the event of any business process disturbances or events, whether due to natural disasters, infrastructure or IT failures, each passport agency relies upon CA for contingency operations and business process recovery instructions. CA is fully prepared to provide direction to the passport agencies.
- ***Diplomatic Security Offices***: The Department's 21 Diplomatic Security (DS) offices currently maintain business continuity and contingency plans in support of three critical missions, (1) to protect visiting dignitaries, (2) to support the needs of those dignitaries and (3) to perform security clearance investigative services on behalf of the Department. In the event of failures or disruptions, DS is prepared to temporarily suspend investigative services in support of its other two priority functions. The Bureau of Diplomatic Security will centrally coordinate all contingency operations from Washington.
- ***Financial Processing Centers:*** To ensure the Department is able to pay employees and vendors, in the United States and around the world, the Bureau of Financial Management and Policy (FMP) is continuing to develop and refine thorough business continuity and contingency plans. FMP provides business continuity and contingency plans for its financial processing centers in Paris, Bangkok and Charleston, but for all overseas posts in making financial disbursements.

Global reporting tools and methods can be used to support current operations

For the Y2K rollover period, the government developed a robust global reporting structure which can be leveraged into a mechanism for monitoring threats against critical infrastructure elements. For example, within the Department of State, we developed a web-based, geographic information system to collect cyber-threat information from all overseas posts. This tool, while developed specifically to support reporting from information system security officers (ISSO) at post during the Y2K rollover, will continue to be used beyond the Y2K window. The tool, called the ISSO Security Monitor (ISM), automates existing reporting functions for ISSOs at post and

aggregates worldwide cyber-threat status information for State's Cyber Threat Team (CTT). (See Attachment A for a sample of screen shots from the ISM tool)

The ISM has quickly become a key part of our cyber security monitoring processes and will continue to be enhanced as these processes change and mature. This is one example of how, through the need to address the Y2K problem, the government has developed global reporting methods and technologies which will continue to be leveraged into an agency's daily operations after Y2K. And, as in the case of State's ISM, these tools could be shared among agencies and used as pilots to support routine business needs across the government.

Unprecedented public and private sector cooperation allowed federal programs access to best-of-class experts

Y2K preparation efforts increased the level of cooperation and coordination between the public and private sectors. In many instances, federal project managers were able to gain access to business sensitive or propriety tools and techniques rapidly. Federal agencies were able to obtain information and subject matter experts in a variety of Y2K-related areas without the need to navigate through the typical bureaucratic obstacles.

Additionally, Congressional support, in areas such as minimizing potential Y2K litigation through Good Samaritan legislation, provided the private sector enough legal protection, to be open to share new ideas without typical warranty ramifications.

This same working level teamwork will be required to effectively implement Critical Infrastructure Protection plans.

Y2K Critical Success Factors / Critical Infrastructure Protection Critical Success Factors

Although there were a number of lessons-learned which could be transferable to CIP/Security related projects, the two primary areas which I believe allowed the federal government to successfully overcome widespread Y2K problems in the face of an immovable, tight deadline standout. Specifically, these include the following:

- The ability of federal Y2K programs to rapidly obtain, and more importantly retain, adequate separate supplemental funding specifically designated for Y2K allowed each agency to acquire the resources necessary to achieve time sensitive objectives.
- Continued participation by key congressional oversight organizations provided federal Y2K programs the authority needed to push agency resources to their limits.

Constant involvement and oversight by Congress allowed federal CIOs and Y2K Program Managers the leverage and authority needed to complete daunting Y2K tasks, for the most part, on time. Reviews by GAO, OMB, and Inspectors General provided reinforcement to top agency leaders that actions and strategies which we believed were needed to achieve our Y2K goals were valid. Without this constant government–wide pressure, I believe most programs would

have fallen short of intended goals -- not due to lack of interest, but due to competing and changing requirements constantly forcing us to prioritize, and re-prioritize our efforts.

As well, the ability of federal agencies to have access to a congressionally managed, yet continuous funding stream designated specifically for the Y2K effort, allowed federal CIOs and Y2K Program Managers the ability to acquire and retain qualified resources in the needed quantity. No longer did the CIO have to fight two battles: fight to get the money into the agency and then fight to keep it.

Critical Infrastructure Protection programs require the same approach. Involvement by Congress and other oversight organizations to raise the level of awareness and visibility throughout the federal community and oversee CIP implementation progress in support of national security goals is vital, and this activity is already underway. But just as important to me and my colleagues throughout government is access to funding which allows each of us to begin developing and implementing our plans in accordance with PDD-63 and other Critical Infrastructure Protection guidance and statutes.

One of the key obstacles preventing agencies from immediately pursuing CIP initiatives is the lack of current funding for these projects. Due to the federal government's budget cycle, forecasting for future work is done two years prior to the budget year. Therefore, as new requirements are levied, current agency budgets do not reflect changing priorities and requirements, such as the new Critical Infrastructure Protection implementation initiatives.

In light of this, there are numerous events that have prevented agencies from adequately addressing current CIP implementation requirements in their FY2000-1 budgets. Specifically, these include the following:

- The need to assess the implications of and begin implementing the ten programs that are part of the recently released Critical Infrastructure Protection National Plan.
- The unprecedented and unforeseen growth of Internet use and technologies over the last two years in both government and industry.
- The corresponding collateral growth of the cyber underworld during this same time period with a seemingly infinite amount of resources.
- The current budgets for Critical Infrastructure Protection don't reflect the challenge of the unprecedented growth of the Internet and the increased threat of cyber terrorism that accompanies this growth.
- United States Citizen's recent dependencies on business processes provided by federal agencies via the Internet.

These are just some of the reasons why federal agencies are poorly positioned to successfully implement Critical Infrastructure Protection programs to address the challenges posed by the ever-growing cyber underworld, not to mention to be in compliance with Executive guidance.

It is my belief, and the belief of members of my subcommittee and CIOs across the federal government, that in order for National CIP initiatives to be fully successful, continued

congressional support and the ability to gain access to separate supplemental CIP and security-related funding, is vital. To reflect the increased requirement for security and the unforeseen growth and corresponding threats to our critical infrastructure, this funding stream must indeed be separate and supplemental – it cannot be an offset to core funding as this will defeat our ongoing operations and maintenance activities. I cannot emphasis enough that without Congressionally backed support, including adequate funding, we of the subcommittee on Critical Infrastructure Protection believe the federal government will significantly fall short of national Critical Infrastructure Protection goals.

Mr. HORN. We are sure there will be questions for every witness. I am going to start with the cochairman of the task force, the gentlewoman from Maryland, to begin the questioning. It will be limited to 5 minutes by each Member, and it will alternate between those who have not had a chance, starting with Mr. Turner after the gentlewoman from Maryland.

Mrs. MORELLA. Thank you, Mr. Chairman.

You know, I hear from all of you some of the same results assessments. First of all, you became more familiar in your various agencies, departments, groups with whom you work, with information technology and its role in the future. Second, there was an assessment of the systems that you have, so you are ready to move ahead with information technology.

Also, I think, rising to the forefront is the concept of the partnerships, partnerships within the Federal Government, the executive branch, legislative branch, but also partnerships with the private sector, partnerships with local governments. I think that is something that we could all learn from and hope to continue to preserve.

We also—I think you all said you felt this was very important and that it did prevent some big problems.

My two questions I am going to meld into one because of the time constraints. First of all, I am surprised myself that there weren't some problems with the Pakistans of this world, Russia. They didn't seem to have any major problems. These are places with older computer systems. I just wondered if you all were surprised at the lack of the problems we have heard about emanating from those countries and other countries that would be in the same category?

Second part, as we look to leap year, February 29th, do you foresee any major or minor problems? Is there something we should be doing about that?

I guess I could start then with Chairman Koskinen.

Mr. KOSKINEN. Well, as I noted in my testimony, I think things did go better abroad than anyone had expected. Partially, though, I think that is because we fell prey to what I thought people did here, which is we didn't believe other countries when they gave us their progress reports.

In the last 2 months of the year, country after country issued reports that didn't say there wasn't a problem, but basically said they identified the places where they needed to apply resources; they had done that effectively and they were prepared. We all sort of said it was late in the day, are they really prepared? It turned out they were, for a number of reasons that I discussed.

One is, a lot of them had much less reliance on information technology, certainly in their infrastructure, than we do here. In fact, I think there are a relatively small number of countries in the world that have complicated computerized control systems for their infrastructure that put them at risk. So a lot of countries discovered that the embedded-chips did not create a problem for their infrastructure.

In fact, in the last quarter of last year, we noted, based on testimony and information from industry experts, that it was unlikely that the lights would go out anywhere or that a dial tone would stop anywhere, that the risk in infrastructure systems with embed-

ded systems was gradual degradation of service over a period of time.

So in the countries that we knew were in the middle—the truly developing countries have very little IT and were at risk primarily in financial systems, it was the Pakistans, Indonesias, Russias, Chinas of the world—that had a reasonable reliance on information technology, where people were concerned about how much they had done.

I think it is a combination of the fact that they started late, but they spent a lot of time in the last 6 to 9 months working hard on it. They got the benefit of learning from everybody else. There was a tremendous amount of information exchanged as we moved through it, and third, a lot of their systems are still analog, they are not digital. They did not depend upon new digitalized equipment, and therefore, they were able to prioritize their resources in a much more focused way.

But I would emphasize that the image of those countries, as if they didn't do anything, they were unconcerned and just waited around, was wrong. We met with 173 country delegates in June at the United Nations, and every one of those countries understood this was a problem that, in some degree, affected them. Every one of those countries was then focused on Y2K, every country met at least twice in every region of the world cooperating, or most of the countries did, cooperating, sharing information.

So I think what happened was in that last 6 months far more work was done in a very focused, effective way than any of us were able to get a window on.

With regard to February 29th, it has turned out in testing, certainly in the Federal systems and in the private sector, that there have been more mistakes than one would have thought. You would have thought people would have gotten the right result for the wrong reason, which is, they didn't understand the rule of centuries, they just divided by 4 and figured out the year 2000 was a leap year.

It turned out there were a reasonable number of programmers that had just enough information to be dangerous, which is, they knew centuries generally aren't leap years, they just didn't know the rule of the exception divisible by 400.

So this is primarily a software problem, although there were some potential embedded chip and system operations problems. Our judgment is we will see no more glitches than we saw on January 1, which were relatively minor and modest.

We are going to monitor it for two reasons. One is we think it is important for those who are operating systems to understand it is a real problem and there is still time for them to test their systems. Most major companies have already done that.

Second, it will be important to monitor the 3 days: the 28th, 29th and 1st of March, so the glitches that occur, and I think inevitably there will be some, are put in the appropriate context. If we had not been able to identify the limited nature of the glitches as they occurred over that first 2 or 3 days on the rollover, we would have had a very different media response. When reports came in of legitimate glitches, the fact, we were able to confirm their accuracy, but expand by saying that is the only country in which it hap-

pened, or the only area that happened. It allowed us to put the glitch in the right context. Absent that, you would have had a greater likelihood of unnecessary overreaction by either the media or the public. We don't expect there will be many glitches, but we think it is important for the public to know where they are and what their significance is.

Mrs. MORELLA. I would like to give you opportunity to respond, Mr. Burbano. Incidentally, I love that acronym for the critical infrastructure, CIAO. It is easy to remember.

Mr. BURBANO. Thank you. Working at the State Department, I had a great opportunity to actually go overseas to many of the countries and meet the John Koskinens of those countries and their sector leaders. I found two things quite interesting, and that is why I personally wasn't too surprised.

One is in talking to them, I found out they were not as automated as some of the people thought they were. But more importantly, the culture in a lot of these countries is not to report the status of government systems, whether it is good or bad, believe it or not. But they will reveal more orally, which obviously when you try to track status, is the only thing that are looked at is written, and if you don't have information to provide, you assume the worst, and that is why they don't get reported as well. Those were the two reasons I found.

Mrs. MORELLA. Like people say about the President, underestimate so that the results will be attributed to you, however it comes out.

Mr. HORN. I thank the gentlewoman.

I now yield to the gentleman from Texas, Mr. Turner, the ranking member, 5 minutes for questioning.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Koskinen, I don't know if you have this information or are set up to collect it, but earlier we had a lot of dire predictions about lawsuits being filed all over the place regarding Y2K problems, and I would be curious as to whether or not any of that has occurred and the degree to which that was a significance problem?

Mr. KOSKINEN. Well, some of us maintained last year that you couldn't have massive lawsuits without having massive failures, and therefore, at least the President Council's position was there was not likely to be this flood of litigation, because there was not likely to be a flood of failures.

That turns out to have been correct. There have been a relatively modest number, but significant lawsuits have been filed where people are arguing about who is going to pay for the fixes, and the question is whether insurance policies cover the failures that companies avoided, particularly in major companies in the United States.

But as a general matter, in the absence of any very significant Y2K failures since the 1st of the year, obviously, you can't have a lawsuit if you don't have somebody damaged in some way. So at this juncture, the only lawsuits out there are primarily focused on arguments between those who fixed the systems and primarily their insurance companies about who ought to pay for it. Even that is not anything like a flood of litigation.

Mr. TURNER. As I recall, of those issues that you mentioned regarding who should pay for fixing, it was not the subject of the litigation nor the success of the legislation that attracted so much attention in the Congress, because all issues were separate and aside from the issues that were dealt with in the Y2K litigation.

Mr. KOSKINEN. That is right. The legislation that the Congress passed primarily addressed the rights and responsibilities of potential plaintiffs and defendants if there were system failures, focused primarily on giving potential defendants the opportunity and the right to fix any of those failures within a defined period of time, and again, since there have been relatively few of those problems that amounted to much, there have been a lot of glitches along the way, there hasn't been much need for the legislation. But I am sure people would argue that since there were great risks, if we didn't get the work done, that there would be failures, there was some potential that the failures obviously would have generated litigation. The fact that we haven't had the failures has had the side effect that we are not going to much litigation.

Mr. TURNER. That is all I have, Mr. Chairman. Thank you.

Mr. HORN. Thank you very much.

We are in the question period. Does the gentlewoman from Illinois have some questions? The gentlewoman is recognized for 5 minutes.

Mrs. BIGGERT. Thank you.

As far as what is going to happen in the future, will there be a plan like continuation of your Council, or is there going to be an office that will remain after probably the leap year?

Mr. KOSKINEN. Well, if there is, it won't have me in it. No, the Council will, as I noted, fold up its tent and fade away into the dusk, probably by the end of March. The issue going forward that Mr. Burbano noted that people are focused on is how will we deal with information technology security and threats to the critical infrastructure, and there is a Presidential decision directive, PDD 63, that sets out a structure and an organizational framework for dealing with those issues, coordinated by the National Security Council out of the White House. So that operation, while we have been coordinating very closely together over the last 2 years, will continue, but it is already set up in the Critical Infrastructure Assurance Organization [CIAO], as Chairwoman Morella noted, and that will be separate from the President's Council.

Mrs. BIGGERT. So there will no longer be a CIO czar?

Mr. KOSKINEN. That is right. I never saw myself as the CIO czar. The CIOs actually have been very capable of taking care of themselves.

Mrs. BIGGERT. Again to Mr. Koskinen, what was the biggest surprise of the rollover?

Mr. KOSKINEN. Well, if you look back at our quarterly assessments, we did four of those. In the last one we put out in the fall, basically in the United States the rollover went as we predicted. We said there were going to be no national infrastructure failures, there would be no regional failures, if there were any failures, there would be isolated problems at the local level. That is what we basically have seen. So in the United States we have been pleased that there haven't been more visible problems for small

businesses. A number of them have had glitches, but they seem to have been able to deal with those, because that was an area we were concerned about.

So, like others, I think the bigger area of uncertainty for us was what was going to happen abroad. Again, we did not think as we noted in our report and in a report by the Department of Commerce that any glitches abroad would have any significant or noticeable impact on the American economy.

We looked at the range of possibilities, where the countries were that were at risk, and where our trade and business partners were, and it was clear to us, no matter what happened in the countries we thought were at risk, it was not going to have an economic impact on us. That also turned out to be true.

But as we discussed earlier, I think all of us were, primarily for a lack of information, concerned about a number of countries that rely on some information technology who started late, where it was hard to know exactly how much work they had gotten done in the last 6 to 9 months of 1999. It turned out that in their basic infrastructure, I think primarily because it was not as much at risk as we might have suspected, there haven't been any infrastructure failures.

The other thing to bear in mind is in the areas where I think they were at greatest risk, which is in financial transactions and communications, those systems were being tested and worked on for the last 2 years on an international basis. So even in a country that didn't have an organized process for infrastructure protection, its banking system had to be testing and working with other banking systems, because the central bankers around the world for the last 2 years focused on that. That was, in many ways I think, the biggest risk they had and the biggest success they had.

Mrs. BIGGERT. I guess just one last question, that so many valuable lessons came out of the experience, and how are we going to ensure that these lessons aren't lost if we don't continue on after leap year day, February 29th, I guess it is?

Mr. KOSKINEN. We created in my prior incarnation, with the help of this committee and others, the Clinger-Cohen Act and the Chief Information Officers Council and CIOs in all of the agencies, with the idea they would be as they have been the focus for information technology issues across the government.

That council is chaired by my successor as the Deputy Director for Management at OMB, and independent of the information technology issues, the security issues that are under the critical infrastructure assurance organization, but focused on by the CIOs as well, there is an existing vehicle that I think, over the last 3 years of its existence, has turned out to be very effective for bringing together all of the Federal agencies and their senior information technology people to work together on isolating and identifying what are the critical challenges the Federal Government faces, how should we be organized to deal with those, and then implementing those situation suggestions.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Thank you very much. Let me ask you, Mr. Koskinen, you have had a lot of experience in the executive branch, first in OMB and other consultant operations, and, of course, this. You

note in your formal statement here, and you mentioned it also, I believe, in your oral summary, this is the greatest management challenge the world has faced in the last 50 years. I think there is probably a lot of truth to that on the world.

But when we look at major management challenges within the executive branch over 50 to 60 years, we see the atomic bomb and the hydrogen bomb, major challenges of how you put that together; going to the moon is certainly another one, setting a goal as President Kennedy there; Admiral Rickover and the nuclear Navy, where you cut through a lot of bureaucracy and got the job done.

I guess I would ask you, as you look here, how do Presidents best get served in dealing with those management problems and the one you just presided over? So give us a little insight into that.

Mr. KOSKINEN. Well, as I say, I think the difference between the Y2K problem and the other significant challenges you floated, which I think were important for the country is, this was a challenge that affected every system in the Federal Government, every agency. So it was not a question of having NASA or the Energy Department or someone else focusing on a very major challenge.

This was a challenge of having every Federal agency, large and small, challenged at the same time, not only within each agency but across agency lines. The Treasury Department services and provides financial services to a wide range of Federal agencies, for example.

I think in all of those cases, what is needed is for people to identify the problem and for it to have a high level of commitment and attention from the Congress as well as from the executive branch. Again, I think the structure set up of the CIO council for information technology challenges going forward is an effective structural vehicle for the government to be able to surface what the issues are and deal with them effectively.

So as we move forward, I think information technology is not a series of episodic challenges for us. Information technology is an ongoing issue, not just for the Federal Government, but for the private sector and world as we become more reliant on information technology for everything from communication to financial transactions.

Mr. HORN. What do you see based on usual experience as to the one or two management challenges after this is done? What do you see? You have had a real eye-opener, I think, throughout the last few years.

Mr. KOSKINEN. Clearly information technology is a challenge. I think it has affected our ability to modernize systems across the government, to have them implemented and operate effectively, has been for some time and will continue to be a challenge.

I think performance measurement. I was a great supporter of the Government Performance and Results Act. I think it is important, not only for effective management within the government, but for an improved dialog with the public about what our goals are and our objectives are and how we are doing and achieving those.

So as we go forward, I think we have on our plate significant challenges, and we probably don't have to reach out and find new ones. If we could handle both of those effectively, deliver services more effectively under GPRA and provide improved updated mod-

ernized information technology delivery systems across the government, I think we are headed in the right direction in those areas, but I think they are major challenges.

Mr. HORN. We are going to be holding hearings with the Government Management Subcommittee on Clinger-Cohen that was mentioned, which came out of this subcommittee and the full committee, and also on the computer security issue, which came up here, so we will be looking for you to testify on those things. Those certainly cut across different agencies within the executive branch. We have a whole other agenda also we can get into with whoever is in place there with the CIOs, because I think that is very important, what you did when you took the job and came out of retirement. You went around and sat down with the Deputy Secretaries who often operate the departments, and I think that was very important.

Would you like anything else to have done that you didn't have time to do?

Mr. KOSKINEN. No. Oddly enough, this was my feeling even before we had the successful transition, if I had to do it over again, I wouldn't do anything differently. We did all we needed to do, I think, and all we could do. I got tremendous cooperation from not only the leadership in all of the Federal agencies, but as I noted, I think a stunning achievement by career public servants in the Federal Government and State and local government, demonstrating an ability to meet a real challenge and meet it effectively.

Mr. HORN. What are you going to do with that $50 million headquarters? Who moves in?

Mr. KOSKINEN. That includes the operational cost for a year, so not all of it will be in place. But OMB is working with the agencies and I have said that when we do our last briefing on March 1st for the rollover, OMB at that time will announce exactly what its plans are for the operational capacity at the information coordination center.

Mr. HORN. Most Presidents early in the morning get a national security briefing coming over from CIA. Do any Presidents ever get a management briefing in the morning as to what is going on in the executive branch and why not?

Mr. KOSKINEN. That is not in my jurisdiction at this point, so I can't tell you whether that is done or not.

Mr. HORN. It was in part when you were Deputy Director for management. The question is most Presidents don't know what is going on in the executive branch unless there is some crisis that hits the papers. Shouldn't Presidents also be looking at the domestic situation, just as they look in the morning at the foreign situation?

Mr. KOSKINEN. There is no doubt that our ability to manage the vast organizations we have and the significant funds that we have is an important part of our responsibility to the public, and I think that not just in the executive branch and the Congress as well, it is oftentimes more exciting to talk about new policies or new programs or failures isolated.

It is much harder, as you know, in the leadership you have had in your subcommittee, to get people to understand and focus on day-in and day-out management. But when push comes to shove,

our ability to make changes and provide benefits to people depends on our ability to manage programs effectively. Good ideas poorly implemented are actually very ineffective.

Mr. HORN. I am going to yield now to Mr. Wu from Oregon for 5 minutes of questioning.

Mr. WU. Thank you, Mr. Chairman. I am just going to use a little bit of my time and really focus on this a little bit more with the private sector panel coming up. I just want to ask one question:

With the upgrades, the new equipment, the other preparation work which was done in the Federal agencies, do you see, or are you currently experiencing a dip in procurement as a result of the bulge, if you will, prior to December 31st?

Mr. KOSKINEN. I think the agencies can probably answer that question better.

Mr. BURBANO. I would like to address that as the CIO for the State Department. I would say not really, for this reason. There was a lot of systems, and I know at the State Department we put a moratorium on systems development and implementation and so forth if it wasn't Y2K-related.

So all of that was put on the shelf, and now it is getting off-the-shelf as soon as the leap year is over. So that is going to offset.

Mr. ROSSOTTI. With respect to the IRS what really happened is that over a 2 to 3-year period, we made an investment to bring up-to-date our hardware and operating system software. But, for example, with PCs, personal computers, we really need to be on about a 3-year replacement cycle there, so we are replacing each year about one-third of the computers representing what was installed 3 years ago. That is kind of the way that we are planning it.

There will be some dropoff in a few areas where we had to make some special investments, but, on the whole, what we really want to do is get on a long-range planning basis where we invest a certain amount every year so that we don't get behind as badly as we were 3 years ago.

Mr. WU. And with respect to personnel, the people you brought aboard, whether on a long-term basis or on a contract basis to help you with the Y2K problem, are they being redeployed within your agencies, have they left? What is going on with the people?

Mr. ROSSOTTI. Speaking for myself and the IRS, what we have done is we simply made a determined effort 2 years ago to retain the people we had. Unfortunately, we were suffering attrition. So we made some very successful efforts to retain the people we had, the people who really know some of these old software systems, and simply had to put many, many other things on hold. We even had to go to the Congress when they passed the Restructuring Reform Act, and ask that some of the effective dates for the law be extended out to 2001, because there was no way to implement some of the things while still working on the 2000 fixes. So what we did was we simply took our staff, tried to retain it, and allocated it to fixing Y2K as the top priority, putting other things on hold. What we are now doing is trying to dig out from this huge backlog.

Furthermore, we are in an unusual position in that we are now just embarking on an enormous technology modernization program. What IRS has right now is we have relatively new hardware in

most cases, and relatively up-to-date operating systems, such as your Windows-type operating systems and your mainframe operating systems.

What we don't have is up-to-date application software. We have, in fact, extremely obsolete applications software, and we have a lot of it. So our role now over the next several years is with the help of a prime contractor is to reengineer that technology, and as I mentioned in my opening statement, that involves business change as well as technology change. So you could almost think of Y2K as just laying the groundwork for what we really have to do over the next several years to reengineer our applications.

Mr. BURBANO. From my view at the State Department, with the new Y2K initiative, if you want to call it the critical infrastructure protection I have been talking about, there is going to be a huge demand for new people with possibly different skills for computer security, cyber terrorism and so forth. So there will be a replacement. Some of the skills used in Y2K can certainly be applied. Others, maybe not. So you have to look at it on a case-by-case basis. Regardless, there is going to be a huge demand for this new initiative that is facing us that is very serious.

Mr. WU. On net, do you think you are adding folks in the hardware-software information systems area, or are you shedding a few now in the State Department?

Mr. BURBANO. I think it is a combination. Not with employees, with contractors. It is a combination of shifting, replacement of skills, keeping some. But don't forget, we are still not out of the Y2K window until the rollover of the leap year. So that is a little bit too early to say right now. But we are starting to look at it in that view, that since we do have this new huge initiative that is very important and will go on for the unforeseeable future, there will be a replacement of skills, and some of those will be applicable and some not.

Mr. WU. I thank the witnesses. Thank you, Mr. Chairman. I yield back the balance of my time.

Mr. HORN. The gentleman from Washington, Mr. Baird, 5 minutes.

Mr. BAIRD. No questions.

Mr. HORN. Mrs. Biggert, the gentlewoman from Illinois.

Mrs. BIGGERT. Thank you. In making the fixes on the computers, organizations really used a lot of different methods, and some, apparently, I think what we heard before were like short-term fixes as far as the date change of windowing, making the dates like 99 and 00 rather than 1999 or 2000.

Will there be any oversight or will organizations, do you think, pursue a permanent change, or will these temporary changes or fixes really last for the long time, or will there have to be something done there? Is there any oversight, I guess, is the question or do they need to—do you know of organizations that will need to pursue the permanent fix? Maybe Mr. Willemssen.

And one other thing, I think, like HCFA delayed putting in a new system until this was over. Do you see that the Y2K will have benefited how for them to pursue that, the new changes in their systems?

Mr. WILLEMSSEN. First of all, you are correct, many organizations had to use techniques such as windowing, because in many instances they had no choice. There wasn't enough time to go through a full date expansion of the software and data bases. So many of them did use those kind of techniques.

They will not last forever. Many of those same organizations plan to have new systems over the next few years, so that the risk, if those new systems come in, is relatively small. However, the caveat to that is when programmers put in 2 digits in the 1970's and 1980's, they thought their systems also would be replaced, and many of them were not.

So there still has to be some oversight of that issue. I would say it is very difficult, though, to generalize among agencies because even within a specific agency business function, some may have windowed, some may have gotten a new system, while others may have fully expanded the date field. It is therefore, an issue where you have to go in and do a full examination and know what you are dealing with and be aware of where your risk points are as time continues with these kind of patched systems.

Mr. BURBANO. I would like to say that at the State Department, since the Y2K program office was run underneath the CIO, which is remaining, we do track where we used windowing. We used a combination of windowing repairs as well as replacements. We do have a list of those. We are tracking them, and most of those are 10 years or more out. But we do have a list of those and we will track them so long as the CIO office lasts.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Thank you. Now the cochairman of this task force, Mrs. Morella, the gentlewoman from Maryland.

Mrs. MORELLA. Thank you, Mr. Chairman. A question for Mr. Willemssen. GAO recently reported that some of the Y2K remediation that was done at Federal agencies was contracted out to private corporations, and in your report, you noted that some of the private companies used non-U.S. citizens to work out the remediation. I just wondered if you would comment for the record on what you found and what you think implications are, if any?

Mr. WILLEMSSEN. We did have a request from the full House Science Committee to look at the use of foreign nationals at the Federal Aviation Administration in both the remediation of software and in the post-remediation review of software that had been previously remediated, and we did find some oversights on the part of FAA. To the FAA administrator's credit, she aggressively took action on these oversights, and they are now in the process of going out and making sure that all of the individuals who worked on the code are indeed checked out. FAA did not know for sure, for all of the systems that were remediated and reviewed, that the individuals had an appropriate background investigation, and therefore whether the risk was manageable in terms of manipulating the code.

So there were some issues that we did find. Again, to FAA's credit, they have been very aggressive in following up on these issues. One of the issues I think you pointed out at one of the prior hearings, was that there was a security risk involved to the extent that it wasn't managed with all of this push to get Y2K done. That it

would be done quickly, losing sight of some of the necessary controls, and that is in fact, what happened here at FAA. All the controls were not in place to check out all of the individuals working on the code.

Mrs. MORELLA. Do you feel comfortable that this has then become a symbol for what could happen if you don't have proper implementation of the regulations and that the agencies all know this? Did we learn from it, besides the FAA immediately saying we will correct the oversight?

Mr. WILLEMSSEN. I hesitate to generalize because FAA is the only agency where we went into depth on this particular point, so I hesitate to say that other agencies may have similar issues, although I know the executive branch is looking into that.

I know that, as I mentioned, FAA has been very aggressive and actually we are expecting a more detailed report from FAA within the next couple of days on all of their actions in response to a recommendation to do the background checks on individuals working on the code.

Mrs. MORELLA. I think you would like to comment on that.

Mr. BURBANO. Yes. The State Department, we looked at this issue very carefully at the beginning. First of all, domestically, we did not use any foreigners, especially that is where mission critical systems are. We do require, regardless, we do require all of our contractors and employees to go through secret clearances. In addition to that, some minor systems overseas did have some FSNs, foreign service nationals, working on their systems, but they were closely supervised by the Americans at the Embassies, and we have had no problem at all. Everybody goes through a clearance check anyway.

Mrs. MORELLA. Splendid. Thanks for that assurance.

I yield back, Mr. Chairman.

Mr. HORN. Thank you very much. Let me ask a few questions here in closing with this panel. I would like the commissioner and Mr. Koskinen to respond to this.

The question would be the extent to which windowing was used to repair systems, and is that really a permanent situation, or how do you feel about the windowing aspect where you are trying to piece it altogether and fool it, shall we say, in terms of the computers?

Mr. KOSKINEN. I don't think anybody has the capacity to tell you how much of the work was done by windowing and how much was date expansion. Windowing is a technique that is effective as long as you don't care about when people were born or transactions in those windows. In other words, if you really are only worried about relative dates, you can window. But in things like Social Security, you can't window very effectively, because you care very much about whether or not somebody has been born on one side of the window or another.

Second, I think the point Mr. Willemssen made is important, and that is, when we talk about configuration management and better control of IT systems, obviously monitoring the way we fix systems for Y2K as we go forward is an important part of that management, and I think it is exactly right to note that 25 years ago, 15 years ago, people working on systems that knew they weren't going

to be Y2K compliant were comfortable because they thought those systems wouldn't be operating. So you have to be a little worried about anybody saying today, well, my windowing works until 2015 or 2023, so I don't have a problem, because those dates will come before we know it.

So I think the answer to that is not was it done, it clearly was done. It was a very effective technique, it was cost effective, and particularly if you are going to replace or upgrade those systems, it was probably the right way to go. It will turn out to be a mistake if you lose track of it, continue to run the systems through the window, and discover you have got a major challenge down the road.

Mr. ROSSOTTI. I am pleased to say in this case, one of the few occasions I can answer very easily, we did not use windowing at the IRS, we did everything with 4-date digit expansion and required a special exception from the CIO to have any exceptions, and, to my knowledge there were just maybe a very tiny handful, maybe one system given an exception. Interestingly, the reason for that decision was not primarily because of worries that would, you know, become obsolete in 10 or 20 years, but because we had so many heterogeneous systems that had to work together, we were not convinced that if we used some windowing here and some data expansion here, that we wouldn't run into incompatibilities among our own systems. So we made a decision to keep it simple, and so everything was made compliant by four-digit date expansion.

Mr. HORN. OK. Now it has been mentioned on the foreign workers in some of the patching up of these systems, I would be curious how you all think how vulnerable our computer systems are as a result of the Y2K, and are you concerned that those remediating systems could have engaged in acts contrary to the best interests of the government? So I would just appreciate—let's start with Mr. Burbano.

Mr. BURBANO. Yes. In terms of the concern, you should always be concerned, but because of the process I mentioned that we took at State with requiring security clearances, all domestic systems, where our mission critical/critical systems are at, only used Americans. We don't have as much concern there.

Overseas, again, I mentioned we did use FSNs who have to be cleared and who only work the minor systems and who are closely monitored by Americans when working on the systems. So we are not as concerned. However, we did develop a project in concert with my sister bureau, Diplomatic Security, on doing some spot checks on some of the systems, just to make sure.

But, just to let you know, you know, even with commercially off-the-shelf systems, you don't know where those systems are developed. They could have foreigners working on those systems also. So you do have to be vigilant about these systems.

Mr. HORN. Commissioner, in terms of computer security, I am sure you have to deal with that every day in some way.

Mr. ROSSOTTI. Well, we have, of course, major security challenges in the IRS from a number of perspectives, including from the old applications software. But I think on this particular issue, that is to say, the contractor support we used for the Y2K, I think we were in pretty good shape on that. There was one particular component of one system that, for a particular reason, was developed with

some offshore people, but that was then subsequently cross-checked by a different group that was cleared. So as far as I know, I think we can be pretty confident on this, we do not have much vulnerability for this particular problem.

That is not the same thing as saying we don't have vulnerabilities for other reasons.

Mr. HORN. Mr. Koskinen, why don't you give us your side of it?

Mr. KOSKINEN. I think Mr. Burbano made the important point, which is, security is an issue beyond Y2K, you ought to be very careful about whoever works on your systems. As a general matter, we were concerned about this issue from the start and we worked with the intelligence agencies and the National Security Council and others, both to warn private sector companies as well as domestic companies to be alert to this issue. Most of them in a large sense are.

Most of the off-shore work was done by the private sector and not the government. Most government work was done by normal contracting, or internal resources, so that there was much less of that done here than in the private sector.

Monitoring what has gone on in the private sector, what has gone on, we have seen very little, in fact, almost no evidence that work done offshore included some kind of security threat. Obviously, the absence of glitches over the rollover means at least if somebody was targeting the time to create mischief, that was not one of those times.

But I think the bottom line to that is, again, as we move forward, information security has to be high on everybody's list. I think, again, the point is well made. It is not just people who have access to your system. It is when you buy systems, whether it is off-the-shelf systems or otherwise, you have to be worried about who worked on those systems, what is in them and what potential impact could they have on your own system. So I think if anything requires eternal vigilance, it will be, in fact, information security and security about those working on your systems.

Mr. HORN. I thank you. We will be holding a separate hearing on the computer security anyhow, so we will postpone the rest of those questions.

Mr. Willemssen, before we round out this panel, I would like you to summarize the following under page 16 of your formal statement, "Reported Year 2000-related Errors in the Federal Government." If you could just sort of bullet them to me in one sentence, each one, just so we have it in the record, I would appreciate it.

Mr. WILLEMSSEN. On page 16 is a summary of what we observed during the rollover from both the perspective of the information coordination center and specific agencies where we were onsite. We tried to summarize what we thought seemed to be significant issues that did come up, even though they were addressed very quickly.

Briefly, those included the Department of Defense intelligence satellite system, the Federal Aviation Administration had some systems with some Y2K failures that again, they were able to remediate and fix very quickly, and the Health Care Financing Administration ran into some difficulties with partners. In one case HCFA had a problem with a bank on some electronic payments

leading to some delays in payments, although it is still within the required targets. Also, HCFA will continue to work aggressively with their providers in making sure that they put forward accurate dates on their claims so that claims are not returned.

Mr. HORN. You say here there are 26,000 claims from providers with these erroneous dates in the first week of the new year.

Mr. WILLEMSSEN. That is why we thought it important to give a sense of the magnitude, because they are not just little things that we are talking about. They are little within the scope of the entire Medicare program, but they do have some impact. But, again, HCFA has done an outstanding job over the last couple of years on getting on top of Y2K. They as much as anyone faced a mission impossible on Y2K, and through the leadership of their administrator, again, they continue to be very aggressive in following up and making sure that the disruptions are kept to a minimum.

Mr. HORN. And then the ones that concern most of us based on our air travel regularly is the low level wind shear alert system. Can you tell us anything about that?

Mr. WILLEMSSEN. Again, those systems were out at about eight locations, but they were out for no more than 2 hours, I think 2 hours 12 minutes at the outside. Fortunately, when they were out, we saw no evidence of bad weather in those locations. So we could be sure, based on the evidence we saw that there were no safety implications from those systems being out. Again, it speaks toward the advantage of all the agencies being poised to respond during the rollover. FAA was ready to get right on top of those systems and fix them immediately, and that they did, to their credit.

Mr. HORN. Yes. I was spending part of that December 31st in the L.A. Tower, and I got a good education from the technicians there. They have a terrific job to do when they are getting those radar sites into operation when something goes crazy with them. I was very impressed by that group.

So are there any other major things that is a worry to the General Accounting Office?

Mr. WILLEMSSEN. I again conclude by saying the rollover was a great success, thanks to the leadership of Mr. Koskinen and yours and Chairwoman Morella's leadership. However, I think it is important that we continue to monitor events over the next couple of months. I would strongly concur with Mr. Koskinen's plan to bring up the ICC again during the leap year, because I think there will be a few disruptions that again occur, and I think there will also be a few disruptions that we start hearing about as processing cycles complete themselves. So we haven't heard the last of Y2K. But I think it will be much, much less than what we had once feared.

Mr. HORN. I want to end on a happy note here and help the Department of State a little, Mr. Burbano. In November 1999, the Department of State submitted its regular quarterly report for the year 2000 to the Office of Management and Budget, and of course, that does come to our subcommittee. After a lot of discussion with you and OMB, it became clear that the language in that quarterly report didn't really accurately reflect the actual level of effort for the Department's independent verification and validation work. Just so we can give you an A on this, please explain to me the

independent verification process that you actually went through but wasn't in the report.

Mr. BURBANO. Thank you very much. At the State Department, one of the things that I did when I came on board in May 1998, as you all know, I came on board, we had straight F's for about a year, so I had to move quickly in order to especially meet the deadlines of Congress. But I wanted to make sure that we did it correctly and not get any surprises at the rollovers. So I set up a very rigorous process where not only did we have the separate bureaus test our systems, but underneath my office, the Y2K office separate from their individual bureau Y2K offices, I had independent contractors test the systems. That was the first level of independent tests.

But in addition to that, I did a partnership with the Inspector General where they would do a second test with their own contractors to review the test and so forth, and certify the systems, along with myself as the CIO. So we went through two levels of independent verification tests, in addition to the testing that the Bureau did themselves.

The misunderstanding that came in that, we were about 66 percent in November or somewhere around that nature, in terms of certification, but when, in fact, it really equalled to about 160 percent, because we had already finished our first level. That is where the misunderstanding came. I think we proved that right since we had really no significant—not only in the mission criticals, but in the criticals as well as the routines, this thoroughness that we did.

Mr. HORN. Well, thank you very much. On that, are there any questions any Member has? If not, we appreciate what each of you has had to contribute to this and the fine work you have done that kept us going with very minor glitches. So thank you all for coming.

We now go to panel two.

Mr. HORN. I would ask you to stand and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The reporter will note all three confirmed. Mrs. Morella will preside.

Mrs. MORELLA [presiding]. Thank you. I want to thank the second panel for being so patient and waiting in going through the first panel testimony and the questions that were asked. So we will be concise. We know that you can offer a great deal to supplement what we learned about Y2K. Proceeding again with the 5-minute rule, you can give us a synopsis of your testimony.

We will start with, first of all, Mr. Harris Miller. I want to comment on the fact that from the very beginning Mr. Miller has been very tuned into this issue, has appeared before this committee probably as many times as any other person who has testified. So we very much appreciate his coming back now at the end as we do our summation and look ahead to the future. He is president of the Information Technology Association of America.

Ms. Kathy Hotka has not appeared before this committee before, so you are the alpha and the omega, the beginning and the end. Ms. Hotka is vice president for technology at the National Retail Federation here in Washington, DC. We welcome you. Thank you.

Mr. Gary Beach has appeared before this joint committee, and he is the publisher of CIO Communications, Inc., from Framingham, MA. Again, thank you for appearing here. Thank you for waiting.

Let's start off with Mr. Miller.

STATEMENTS OF HARRIS MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA; CATHY HOTKA, VICE PRESIDENT FOR INFORMATION TECHNOLOGY, NATIONAL RETAIL FEDERATION; AND GARY BEACH, PUBLISHER, CIO COMMUNICATIONS, INC.

Mr. MILLER. Thank you, Madam Chairwoman. It is said that politics makes strange bedfellows, but I found out that Y2K makes strange bedfellows, for on the morning of January 1st, instead of being snuggled warm in my bed with my wife, I was instead with Chairman Horn at the C–SPAN studios doing a broadcast on Y2K.

What is even more unusual is that at 8 a.m., constituents of his from California were calling in, which means at 5 o'clock in the morning they were paying attention to what was going on with Y2K. But I appreciated working with both of you chairmen and the members of your subcommittee. I am going to skip the victory lap you mentioned, Madam Chairwoman. It is my written statement and will be in record. I obviously want to commend the subcommittees, and particularly Mr. Koskinen, for his leadership.

From the perspective of the private sector, we do believe this is a real crisis that we did face, it was not something that was hyped or made up. In fact, as I was walking down the hall this morning with our Y2K program manager, Heidi Hooper is with me, she noted there wasn't a line about the hallway waiting to get into the subcommittee hearing. I said that is good news, because if, in fact, the problems had occurred, I suggest you wouldn't have Harris Miller and Kathy Hotka and Gary Beach on this panel, you would have Alan Greenspan and Secretary Summers discussing the global recession that had been caused. So, in fact, the fact we didn't have a major crisis is good news, and the fact we don't have hordes of people standing around is, in fact, very good news.

In terms of the magnitude of the effort, I would certainly agree with Mr. Koskinen's effort. In fact, I even go a little more hyperbolic, I think it is the biggest success since the building of the pyramids, because it was, in fact, a global effort, government, private sector, hundreds of thousands of individuals around the globe working together to achieve this success.

To talk about the lessons learned, I would like to refer to what I believe is a Y2K renaissance. What do I mean by a Y2K renaissance? I think it really is two parts. First of all, the rationalization of the existing computer technology. You heard a lot about this from the first panel in the Federal sector, but the same thing was true very much in the private sector. The fact that time and again, because of the necessity of dealing with this huge challenge, companies were able to get rid of deadwood programs, they were able to bring into their companies more modern and more efficient computer systems.

They also learned to do supply chain analysis and in a systematic way that they had never done before. They were able to collaborate in ways never experienced before, either within companies

or across companies. They were able to develop contingency plans, many of which were not needed as it turned out, at least are now in place should there be future problems, and they learned to approach the entire IT system in a much more strategic way.

That is going to mean that down the road these companies and ultimately their customers can take much more benefit from information technology. The productive gains which Mr. Greenspan and others have noted have helped to contribute to the continued growth of our economy and the high productivity should be even stronger because the IT systems in companies as well as within the government are now being treated much more rationally and in a much more systematic way.

The second reason I call this a Y2K renaissance is the new directions that companies are now taking. Because as they came to understand through Y2K the strategic as opposed to tactical importance of IT, they are now moving ahead implementing future IT much more strategically. Obviously, the Internet changes everything, and we are seeing throughout the private sector and we hope the government sector will quickly catch up the use of the Internet for improved, dramatically improved in many cases, internal processes, whether you are talking about personnel systems, whether you are talking about human resources or financial services, whether you are talking about inventory control, all of these basic day-to-day business operations are being done much more effectively and efficiently on the Internet. This is one of the new exciting aspects of Internet technology.

Also, of course, dealing with customers, and customers don't just mean business to consumer, the kind of stuff you read about on the front page, about Amazon.Com and others. It also means business to business, because businesses are also customers, and the ability of businesses to deal much more effectively.

So this is the kind of Y2K renaissance I see coming, because as we come out of what Mr. Burbano and others described in the Federal sector, which also occurred in the private sector, namely, a temporary freeze in many cases on new programs and spending, and now all these projects which have been temporarily set aside are going to be brought out to the fore, and again, I think you are going to see massive increases in productivity, in major benefits to customers, and again, customers I define broadly as businesses and individual consumers.

Let me talk about some other lessons learned. One of the lessons learned that was that while the government sector did an excellent job, as the previous panel discussed, the private sector also did a remarkable job.

Some names of individuals who you may not have come across, or maybe you have come across, like Bill Mont and Tim Shepherd Whalen from Global 2000, or Ron Balls from the ITU, people who are able to take entire sectors and coordinate them, you are going to hear from Ms. Hotka about the retail sector, contributed mightily to the success. I think ongoing we have learned lessons about the ability of these sectors to work both nationally and globally.

I also use that as a point for future global cooperation. The International Y2K Coordination Center, which both of you were very involved with and which Mr. Bruce McConnell headed so ably, has

demonstrated the opportunity for global cooperation. Coming out of that, I am hopeful we will see some continued opportunities.

For example, the International Y2K Coordinating Center steering committee is considering the creation of what is called the Center for Digital Opportunity, which would be a cooperative program to promote Internet growth in developing countries to the same extent that it currently is in developed countries. In fact, tomorrow the steering committee will have a conference call and I am involved in that also, as is Mr. Koskinen, to see about the possibility of building on the linkages that have been established through Y2K in that area.

Similarly, the issue that Mr. Burbano talked about so extensively and Chairman Horn said you will be having further hearings on, the whole issue of information security.

While there are information security issues which are very specific to the U.S. Government, there are many issues which are global in nature. Again, the 170-plus countries that work together through the international Y2K cooperation center should be able to take those linkages which they established and build on them for information security. I think that is also another lesson learned.

The last lesson learned which I would like to refer to, and I am a little bit over my time, is that the Y2K problem was solved without government dictating what the private sector needed to do, without legislation. As you remember, you two chair people, at a hearing early on, there was actually discussion about perhaps Congress having to mandate the private sector to take specific actions. You came to the correct conclusion that, in fact, there were better ways to do that, rather than mandating specific activity. We did get through this without mandating specific activity on the part of the Congress to order the private sector to do activities because the private sector was and to work collaboratively.

I think the lesson learned there is as we move ahead to other challenges in information technology, whether it be the information security area or regulation of the Internet, that the claims that the private sector made to you then that we can handle this in a collaborative manner, not working against government, but cooperatively with government, did prove true in the Y2K area, and I think when Congress approaches other issues, such as information security or other issues of regulating the Internet, they should take that lesson learned, and perhaps it will also prove true that you do not need legislation, that there are other ways to get things done in this new economy and in this information revolution.

Thank you very much for giving me the opportunity to appear before you, and I would be glad to answer any questions.

Mrs. MORELLA. Thank you. I also want to comment on the fact that I did hear that early morning C–SPAN program, and it was very informative. Thanks for your leadership.

[The prepared statement of Mr. Miller follows:]

Statement of Harris N. Miller
President, The Information Technology Association of America (ITAA)
Before the Joint Oversight Hearing of
the Subcommittee on Government Management, Information and Technology and
the Subcommittee on Technology

January 27, 2000

Introduction

Chairman Horn, Chairwoman Morella, and Honorable Members of these Subcommittees, I am honored to testify before your Subcommittees today on the subject of the Year 2000 Computer problems again. I am President of the Information Technology Association of America (ITAA), representing over 400 direct and 26,000 affiliate members in the IT industry across the United States.

I am also President of the World Information Technology and Services Alliance (WITSA), consisting of 39 information technology associations around the world. Through ITAA and WITSA, I have been very involved since the beginning in education, awareness and information sharing related to the Y2K issue on a national and global level. As I had the privilege to participate in the first of the Year 2000 hearings your Subcommittees held, I appreciate the opportunity to testify on what may be the last.

Unprecedented Success Story

As I have testified before to these Subcommittees and others on the Hill previously, ITAA was the nation's Paul Revere on the Year 2000 issue. We began our midnight ride in 1995, with a series of industry meetings and publications. We learned much about the Year 2000 issue along the way, built the industry's only certification program, a weekly electronic newsletter reaching ten thousand readers in 80 countries, an alternate dispute resolution program, a solution providers directory, an information packed Web Site (http://www.itaa.org), and much more. I also gave numerous Year 2000 presentations to groups all over the world, in locations as diverse as Brazil, Beirut, Beijing, Shanghai, Paris, Mexico City and many others in my role as WITSA President, in addition to testimony here on Capitol Hill and speeches to government and industry leaders here in the U.S.

Now that the ride is over, we have, in effect, defeated the British at Bunker Hill. But I must give credit to the many leaders who made the success possible. The Y2K transition in the U.S. and around the world was so smooth in large part due to some of the people sitting in this room today. I commend you both, Chairmen Morella and Horn, for highlighting this important issue and helping to bring it to the forefront of the attention to the U.S. government. Senators Bennett and Dodd were also critical in their roles with the Senate Special Committee on Y2K. I also commend the three witnesses on the previous Panel, John Koskinen, Joel Willemson and Commissioner Rossotti, each of whom had

very prominent roles in assuring that our government and our country were prepared for the Y2K rollover. The appointment of John Koskinen by the President in 1998 signaled the recognition by the Administration of the seriousness of Y2K, and the creation of the President's Council may have been the turning point that enabled our government to utilize time and resources to remediate the government systems in time for the rollover. ITAA worked closely with the Department of Commerce and the Small Business Administration to communicate with the commercial sector on Y2K issues. Those two agencies performed a particularly important task of bridging the gap needed to communicate with medium and small businesses.

This Congress played a crucial part in ensuring a smooth transition to 2000. Combined with the many hearings held by your Subcommittees and others, the passage of the Information Readiness and Disclosure Act of 1998, a bill that ITAA strongly supported, allowed businesses to work more closely together to solve issues together quickly. ITAA worked with our members and non-member companies to explain the provisions of the Act and encourage companies to share information after the bill was passed. The Small Business Y2K Readiness Act was a necessary measure that also encouraged action for our nation's thousands of small and medium-sized enterprises, so important to supply chains across the U.S. These two legislative measures captured the spirit of U.S. success with solving Y2K – information sharing, awareness and special resources where necessary.

We cannot talk of the tremendous success of the Year 2000 transition without mentioning the hundreds of thousands of programmers and engineers who painstakingly combed through trillions of lines of computer code to repair nearly all of the Y2K date references, then tested and re-tested the remediation to make sure it was correct. Also critical to the national success were the CEOs and Boards of Directors who recognized the need to remediate and made it a priority. And finally, the Chief Information Officers in business and government who engineered the successful repairs and also made sure that all supply chain components were compliant, were essential to operationalizing the directions from management and mobilizing the troops for successful repairs.

Remediation was no small task. This was the greatest peacetime mobilization of all time – or at least since the building of the pyramids. But Y2K is also the unmitigated best technology news story of the millennium – and the benefits of the investment of time, resources and new equipment will pay off in real increases in productivity, competency and understanding of technology.

Y2K Renaissance in the Making

Y2K occurred for numerous reasons, in no small part due to the incredible resilience of information technology systems themselves. Many software applications were designed to operate in the "here and now" but instead worked productively far into the future.

Ironically, much software systems became the victim of their own success, tripped up by the two-digit date formatting convention.

I would submit that with the substantial investment made by companies in fixing their systems, these firms now stand poised to reap the benefits of a Y2K Renaissance. How can this be?

Any major organizational change has at least two components: a consolidation of things past and a channeling of time, energy and resources into new strategic directions. We have both elements present with the Year 2000 date conversion. For many firms, Y2K became not only a down in the weeds date find-and-fix exercise, but the pretext for making a systematic, enterprise-wide reassessment of IT assets. In essence, companies decided that while getting the oil changed, why not have the engine tuned also? For the best managed organizations, the "tune up" meant taking a careful inventory of all systems, applications, Commercial Off The Shelf (COTS) products, utilities, databases and other software and embedded system holdings. Programmers and other IT professionals considered issues such as:

- what, where and how frequently corporate IT assets were used;
- how critical these were to operations;
- the extent to which systems and subsystem components were properly documented;
- the interrelationships between systems both inside and outside the enterprise;
- the accuracy of IT inventory listings;
- and mechanisms for managing IT assets.

Through this process, organizations have gained an unprecedented level of visibility into IT infrastructures—a blueprint for managing the installed base and the informational foundation for moving forward. In drawing the lines tight, companies have pruned away the dead wood from their software inventories; prioritized systems and gained new insights as a result; improved the management of source code, test scripts, documentation and other software artifacts; created test beds and logical partitions for system testing along with invaluable new experience in the testing realm; gained bona fides in such areas as configuration and program management; built important and constructive new bridges between IT shops and line units; acquired exposure to many innovative new tools and techniques for software design, development and maintenance; achieved a more quality-oriented approach to software development, leveraging the benefits of formal processes and methods.

Faced with a fork in the road, many companies used the Y2K Renaissance as the opportunity to not just renovate old systems but to replace them altogether. This process in itself has been instructive. Conventional wisdom on new software deployments suggested that years are required to implement an enterprise application. Given the narrow window of opportunity and "brick wall" due date for most Y2K replacements, firms were forced to think long and hard about the wisdom of replacing their legacy systems. Many organizations decided to face the new millennium with new Y2K compliant applications in place. I think that one of the unsung stories of the Year 2000

conversion is the dramatic success enjoyed by those firms able to field new systems so quickly and, apparently, so flawlessly. Advances in technical areas such as common program interfaces, data standards, directory services and other categories are ringing the risks from software projects. Modern programming techniques, including object oriented programming and structured database approaches, have also played an important role.

Another of the success stories shared across the Y2K community is the extent to which companies learned to work together. The Y2K potential for mishaps was recognized and avoided by organizations willing to remove their own organizational barriers and to seek crosscutting solutions. This is certainly true of the find-fix-and-test interplay between IT and line business units, as mentioned earlier. But this is only part of the story. Y2K required companies to think and plan for contingencies on an enterprisewide basis. As a result, employees across a broad spectrum of professional disciplines became involved in the contingency planning process. These individuals gained the opportunity to view their company through a much wider lens and to appreciate its inner-workings with much greater understanding and appreciation. They also received the opportunity to step outside of the box. To see how a corporation is one link in the chain bringing value to customers. They discovered the vulnerabilities posed by supply chain relationships, how these relationships are under girded by information systems, and how the entire business eco-system must be protected by proper communication, knowledge sharing, testing and contingency planning.

Surely these new insights will yield a variety of business and economic benefits, from graduating far more employees to general management to finding new points of leverage for IT solutions, themselves.

So this Y2K Renaissance sets the stage for good things to come. I think its also fair to say that many companies responded to Y2K by freezing new system development activity, putting off plans to build E-business functionality, shying away from new enterprisewide software deployments. With every freeze comes a thaw. The Y2K winter heralds a robust infusion of IT investments, particularly in the adaptation of Web technology to traditional business processes—and vice versa. The Internet is transforming everything about commerce today, from assembling the international team that designs a product to transmitting the truck routing information necessary to bring it most expeditiously to your door. To the extent that Y2K created a freeze, it also gave companies the opportunity to step back and build their post-Y2K technology investment strategies. With the Year 2000 software conversion out of the way, I look for a floodtide of innovative new information systems deployments across the economy.

The Hype and the Reality

I am by nature an optimist and freely admit that this notion of a "renaissance" sees the Y2K glass half full. I do not doubt that there are those who see the glass completely full—of hype. To these individuals I would simply observe the following:

- If left uncorrected or corrected improperly, the Y2K bug would have proven troublesome at best and disastrous at worst. The situation was binary: either fix the software or suffer the consequences. Any doubts should be resolved by the Japanese nuclear power plants reporting glitches with their monitoring systems, the Department of Defense reconnaissance satellite disabled by a glitch on the ground, the medical equipment failures in Sweden and Egypt, a Y2K problem at the Oak Ridge National Laboratory, the Doppler weather system shut down in Chicago or the double charging snafu in Visa and MasterCard transactions. I suggest to you that if just one problem—that with credit cards—had not been properly remediated, you would be listening to Alan Greenspan today talking about an economic downturn caused by Y2K, not Harris Miller talking about success.

- The medium is the message. In this case, the Internet proved to be the great equalizer—an incredibly powerful medium for leveling the learning the curve on Y2K renovation. Both companies and countries coming late to the proceedings were able to gain enormous efficiencies from the shared experience of others. These efficiencies expressed themselves in saved work, fewer mistakes and false starts, more productive processes, a better understanding of available tools and supports, compliance information and more. The Internet was put to wonderful service by industry trade associations, ITAA among others, who used this medium as a force multiplier. Working together, industries from electric and nuclear power to retail and banking closed ranks to defeat the bug.

- We are not out of the woods yet. Y2K to date is an incredible success story. Almost one month into the new year, the outages that have occurred, while many have been significant, have not been of the epidemic proportions once feared. Still, we continue to hear of disruptions on an almost daily basis and organizations still face important date rollovers, including leap year, end of quarter and end of year closings, and other events. While the popular perception surroundingY2K conjured fears of a major and immediate meltdown, many knowledgeable observers have warned of the cumulative effect instead. As with everything else Y2K, only time will tell.

- Industry proved up to the task. The self-governed information technology industry, working in tandem with other industry groups, identified the Y2K threat ahead of time and fielded the solutions necessary to head off disaster. This industry-driven approach worked in real time—a happy circumstance which I expect would have been quite different if attempted under a government regulatory approach.

Key Global Cooperation

One of the very real benefits of Y2K was the global cooperation among governments and in the private sector. Commercially, large companies made it a priority to work with smaller vendors and suppliers to ensure Y2K compliance, whether those businesses were located in Mexico, Madagascar or Mongolia. Among governments, some might argue that such a rapid mobilization by so many has never even been tried before, let alone succeed. Take for example, the nuclear missile command center set up by the United

States and Russian militaries in Colorado Springs to collaborate on weapons monitoring. A remarkable example of information sharing.

I have been fortunate not only to witness this cooperation first hand, but to play a part in its development as well. In 1997, WITSA produced the first global white paper on Y2K impact which was widely distributed among our 39 member associations to generate dialogue and awareness. WITSA, the International Chamber of Commerce (ICC), the World Bank, the Organization for Economic Cooperation and Development, and INTUG then organized the first global summit on Y2K in London in October 1998 for the commercial sector, bringing together key delegates from over 35 countries. For many on the international scene, this was the first wake up call outlining the realities of Y2K, and later international Y2K conferences held were modeled after this event.

WITSA also worked with the leadership of the United Nations to help support the December 1998 meeting of 120 national coordinators in New York City, which called for greater international coordination, information sharing, and cross-sector dialogue on the Year 2000 problem. The meeting also recommended launching a global awareness campaign with emphasis on international contingency planning. The International Year 2000 Cooperation Center (IY2KCC) was established at the beginning of February 1999 to carry out the recommendations of the special meeting, and WITSA was able to play a critical role in its creation by obtaining funding from the World Bank's InfoDev sector to create the infrastructure for the Center. The Center is governed by a steering committee of National Y2K Coordinators, of which I am a member.

Bruce McConnell, the Center's director, and the IY2KCC have been successful in creating a trans-border dialogue and action on Y2K. Through a series of regional and global meetings, the Center outlined concrete action plans in the areas of awareness, cross sector cooperation and cross border cooperation and contingency. Every indication now shows that the cooperative agenda and programs developed by the IY2KCC have helped countries, companies, organizations, and other individuals around the globe cope more effectively with the Y2K challenge.

It is my belief that avenues have been opened and communication lines formed that can lead to new relationships and substantive agreements between countries that collaborated on Y2K. The threat of disaster may have forced the initial cooperation, but I believe the threat of losing connections in the future will keep these lines strong. Too much could be lost by severing ties in 2000 and beyond.

New Opportunities

The high level of international cooperation on important IT challenges should continue in the next Millennium. One of the strongest challenges is that insuring that the Digital Revolution, which has already brought access to the Internet to 200 million people worldwide, does not inadvertently create a divide between digital "haves" and "have

nots." Instead, the Internet should be seen and become a technology, which is available and beneficial to all.

The IY2KCC highlighted the effectiveness of a global dialogue on high technology challenges and opportunities facing all countries and sectors. While much publicity has surrounded the explosive growth of the Internet and e-commerce, there is growing concern that the Internet will develop unevenly and could potentially further the economic divide between developed and developing economies and within various countries between individuals of various socio-economic status. However, not enough has been said or done to maximize the new directions open for both developed and developing countries because of the Internet—what many refer to as the Digital Opportunity

Building on the network of experts developed by the IY2KCC, a global coordinating Center on Digital Opportunity should be created. The Center should include both public and private sector experts. The mission of the Center should be to promote the expansion of the Internet and electronic commerce in developing countries by establishing increased collaboration among governments, multilateral institutions, businesses, and NGOs which want to promote and can benefit from insuring that as many people as possible are connected to the Internet and the products and services that can be delivered thereby.

A second area for future collaboration should be on information security. Like Y2K, so much is at stake as more and more of the national resources of the globe are carried over technology and computers. Threats to systems come in multiple forms: disgruntled employees, mischief-minded hackers, terrorists, rogue nations. These threats are global in scope and global in their potential impact. They are not just problems in the United States. All those who produce and use IT have an obligation to lead in our own countries. Information security is a fundamental challenge that requires everyone's attention.

Chairman Horn, Chairwoman Morella, again I thank you for the opportunity to testify here today, and I would be happy to answer any questions from the Subcommittees.

Mrs. MORELLA. I am now pleased to recognize Ms. Hotka.

Ms. HOTKA. Chairman Morella, Chairman Horn, members of the committee, retailers appreciate your leadership on this issue, and I appreciate the opportunity to appear here with you today.

As you may know, the National Retail Federation's Survival 2000 project worked for 3 years to coordinate a joint retail-industry response to the year 2000 issue. We worked with department stores, restaurants, specialty stores, liquor stores, pharmacists, convenience stores and grocery stores to make sure that you could shop this year. People are really shopping as a result.

How did retailers fare? Better than we expected. But the sector desk at the White House information coordination center that seemed to have the most to talk about was ours, retail and small business. As expected, bigger businesses experienced annoyance grade glitches and some smaller ones found out that that fix on failure policy they had was not such a great idea.

Anecdotally, we know of retailers still processing credit cards manually because of the IC verify problem. One retailer's store credit cards failed. Cash registers at one chocolate store chain would not open. But the examples here are relatively minor.

Now, it remains to be seen whether the global supply chain would be unaffected, larger retailers have some doubt about whether or not we have sailed through this internationally.

Was it worth the work and expense? We already know the answer. While retailers spent multiple billions of dollars to find and fix and replace software and hardware and to conduct extensive testing, we also would not do it any differently. We had conducted a survey in 1997 that showed that if retailers didn't undertake this work, many key systems would simply be dead in the water. We found out that 100 percent, all, private label credit card systems would not have worked; 99 percent of warehouse management systems would have failed. Most retail processes are touched by technology, and our members were not willing to bet the business they would be fine without remediation. My members are astonished that some columnists have questioned the value of the investment. Mr. Burbano mentioned earlier that some countries found they were less dependent on technology than they thought. We discovered we were more dependent on technology than we had thought.

So what lessons did we learn? We learned four:

First, we learned that most organizations underestimated their reliance on IT despite healthy investments in technology, retailers found that some business critical processes were being run by business units on 15-year-old software. You cannot run a company on paradox 1.0 for DOS. It is not a good idea.

Some companies maintained software they didn't need. Some key programs were being run by people with no IT background. Companies did not have contingency plans. In fact, we found only one company that had a contingency plan at all.

In the end, though, savvy companies realized Y2K was not an IT issue but a business issue, and that IT needs the continuing attention of the CEO. Those companies that did best had the CEO in charge of this project. We who lead industries must bring a better appreciation of IT as knowledge management, not just PCs and printers.

Second, we learned that reliable information was hard to come by on this, particularly in the early days. Should retailers have believed technology companies product updates? They seemed to change hourly.

Should retailers have believed government agencies' self-reports? How about suppliers? How about the fear mongers? Ultimately, no self-reported information was reliable, and retailers simply conducted their own verification in the absence of reliable test data or organizational benchmarks, this was our only choice. It was expensive and time-consuming. We know of a number of companies, for instance, that put people on airplanes all during 1999 to check on international readiness. These people simply traveled from country to country.

Third, we learned that government may have a useful role in helping companies use technology as a business tool. There is no doubt, but that the white hot spotlight of your committee's attention to this issue brought home to all of us the need to work diligently. Your contributions to private industry preparedness should not be underestimated. We paid a lot of attention to those report cards. Our friends at GAO published world-class, best-practices documents that gave private industry some models to work from. John Koskinen and his talented staff helped galvanize countries, governmental bodies, private industry and the media. All were key to helping retailers who rely on a global supply chain and public confidence. We thank you all. Like Harris, we believe that this should be a partnership and not a speaking from on high.

But, fourth, we learned that joint action was key. No one retailer did it alone. Fierce competitors worked together to keep the industry ready. Generous companies allowed staff to speak at conferences to spread the word to others.

So going forward, we would like to continue what we have been doing for the past several years, working to protect America's business data. Congress should continue to show interest in America's information infrastructure. The White House ICC where public-private partnerships were so useful might continue to be a valuable tool. Business still needs best practices that can help smaller companies use technologies responsibly, and reliable sources of information about threats to data from hackers, viruses and industrial espionage are needed. Let's continue to work together. Public private partnerships got us through Y2K, but we have compelling reasons to keep working in 2000 and beyond.

Thank you.

Mrs. MORELLA. Thank you very much for that testimony.

Now we will hear from Mr. Beach.

Mr. BEACH. Madam Chairwoman, Mr. Chairman, I thank you for the opportunity to appear before the committee again. Madam Chairwoman, talking about the victory lap analogy, I live close to Hopkinton, MA, which is the start of the Boston Marathon, and I would say what we have learned with all the great work here is that we are in the first mile of a marathon, a marathon showing how pervasive technology is in all of our lives.

The subject of my testimony here is in the written side, but I will orally summarize it, is lessons learned, opportunities created, and

I would encourage the committee to look forward as to what are some of those exciting opportunities.

Increasing the crescendo of hyperbole, we heard about John Koskinen talking about it in the last 50 years, and Mr. Miller talking about the work as is comparable to pyramids. I would say that the year 2000 computer problem and the work that was done on it by a myriad of groups is the most remarkable peacetime example of human cooperation in the history of the world, and I have an idea for you at the end of my oral testimony.

We are entering, what I see, as the age of digital enlightenment where technology is going to help nations govern better, help businesses conduct better business, and make everyone's digital life all the more meaningful.

The committee asked the panelists "was Y2K hyped for profit?" Those of us on the front lines, the ITAA and Kathy and her group and others, have no doubt that without proper remediation and all the great work that this committee has done, Y2K would have had a severe impact on computer systems around the world.

It is interesting, isn't it, that those companies that may have benefited from an increase in sales of computer hardware or software over the last couple of years are now reporting in the Wall Street Journal over the last couple of days saying their earnings reports are down because of Y2K. So what goes around comes around, and it is all going to even out in the end.

So, the long-term legacy of this challenge is going to be akin to the oil crisis that we saw in the mid-1970's, where we had relatively short-term pain, and long-term we had more fuel-efficient cars. The Y2K long-term legacy was simply mentioned here many times today that it caused the world to update its computing infrastructure in a relatively short period of time.

I was personally surprised at how well the rest of the world made it through digitally unscathed on January 1st. I would say this experience was a resounding clarion call to our government and our industries that other nations, many of whom predominantly use U.S. technology, are running neck and neck with the United States. It seems to me that the digital playing field appears to be leveling off. And, in this new 21st century, where the economy is going to be very digital and electronic, these other countries are prepared to provide stronger global competition.

On the earlier panel we talked about foreign nationals. I had an opportunity last year to travel to Bangalore, India, where I saw thousands of workers producing Y2K remediation projects, many for United States firms. These workers are now going to be looking to produce products and services in their own global environment.

The next big technological breakthrough is going to be e-commerce. A CIO poll recently reported that 73 percent of American businesses now have e-commerce initiatives started. What is even more important to me is by 2001, these e-commerce initiatives are going to be the core business models of these businesses.

Shifting to opportunities for government, the Y2K revolution has afforded the Federal Government and the State and local governments opportunities to modernize its computing infrastructure. We should leverage these revitalized systems to better do the business of governing. Opportunities before this House and this committee

in light of legislation continue on Internet taxation, how Americans will govern using technology, closing the digital divide of the have's and have not's, and possibly the aspect of a not too long-term strategy of having the United States wean off its dependence on foreign workers.

I did some work last year in Massachusetts reviewing the State's entire higher education system. While there are more and more men and women entering computer science courses in classes across the country, the challenge is that the faculties at many of these institutions are not prepared to teach the new technologies.

As I mentioned in the beginning of my testimony, I had an idea. I would encourage Madam Chairman and Mr. Chairman to send on behalf of the world's IT workers, a letter to the Nobel Prize committee in Oslo recommending that a special award be given in October to the world's IT workers, where possibly a person from the informatics committee at the U.N. could go to accept it, and on a site, some place on a U.N. URL, any worker who worked on Y2K could download it and proudly frame it in his or her office.

In closing, Y2K in context, was a massive tactical challenge, but what it underscored on a more strategic level is the importance of technology in governing and commerce, and with the seemingly stable technology infrastructure in place, now is the time to take advantage of these new opportunities.

Thank you.

Mrs. MORELLA. Thank you.

[The prepared statement of Mr. Beach follows:]

My name is Gary Beach, and I am the publisher of *CIO* magazine, the leading publication for chief information officers (CIOs) and other senior executives who use information technology (IT) to improve their businesses. *CIO* provides its readers with current information and case studies on the effective uses of technology. Our readers work in major corporations, including Fortune 1000, and in federal, state and local government agencies. My Year 2000 expertise includes daily dialogues with business and technology executives as publisher of *CIO* and my work on the steering committee of YES Corps, an international network of volunteer Y2K experts supported by the International Y2K Cooperation Center, the United Nations and the World Bank. The subject of my testimony is Lessons Learned.

The recent Year 2000 computer problem is the most remarkable example of global human cooperation I have ever witnessed. It brought many organizations together, like the International Y2K Cooperation Center and its offshoot, YES Corps; the President's Council on Y2K led by John Koskinen; the World Bank; the United Nation's Informatics Committee and many others. Perhaps even more impressive are the thousands of business and community leaders who made remediation a priority and approved the appropriate expenditures and the IT workers around the globe who spent an unfathomable amount of time, energy and brain power on planning and implementation over the past few years. Through this experience, the world has entered what I call "the Age of Digital Enlightenment," where technology is going to help nations govern and enable executives to conduct better business. There is now widespread awareness of how pervasive technology is in everyone's lives, not just those of the digital elite.

In June of 1998, the Beach-Oleson Pain Index predicted the majority of Y2K-related problems would appear as minor disruptions and inconveniences as opposed to catastrophic events. You can view the pre-Y2K predictions and probabilities by visiting *www.cio.com/info/releases/y2kchart.html*. Post Y2K, we know only what has been publicly reported, and there is a chance some businesses are not reporting Y2K-related incidents, which, in most cases, are probably minor, or we would presumably be aware of them. Why would incidents go unreported? Most businesses don't have an incentive to come forward with their problems. The potential for spurring stock problems and creating unnecessary anxiety and negative publicity is a strong incentive for keeping quiet. However, there are some incidents we do know about:

- Nine nuclear power plant incidents occurred in Japan, and seven occurred in the United States, all of which were apparently minor electric power supply problems. According to press reports, the incidents did not involve a compromise of safety-related systems or require plants to be shut down. (Source: *The Daily Yomiuri*, Tokyo January 6, 2000 and *The Los Angeles Times*, January 2, 2000.)
- Point of sale credit card companies posted transactions multiple times to credit card accounts, because they did not download an eleventh-hour patch. (Source: *ComputerWorld*, January 17, 2000.)
- The U.S. Defense Department experienced computer failures related to processing imagery from intelligence satellites, which resulted in an interruption in the flow of

spy satellite information. However, the Pentagon insists the trouble did not jeopardize U.S. national security. (Source: The Associated Press, January 14, 2000.)

All of these organizations had gone to great lengths to remediate their systems; if they hadn't, the results would not have been so benign.

The aforementioned examples illustrate the ridiculousness of the recently posed question: "Was Y2K hype for profit?" Those of us on the frontlines, including IT professionals, myself, *CIO* readers and John Koskinen, have no doubt that without proper remediation, Y2K would have had a severe impact on computer systems throughout the world.

Not only could Y2K incidents have been more serious, there was the potential for a myriad of other complications that could have caused problems on top of problems. A few examples that substantiate the reality of anticipated Y2K problems include actual supply chain and air traffic failures. Let me explain:

1. Wind-shear alert systems failed at a number of airports across the nation including Atlanta, Denver, Orlando, Fla. and Tampa, Fla. Computer systems had to be rebooted, which took two hours. (Source: *The Los Angeles Times*, January 2, 2000.) What if aviation experts had been unable to rectify this system failure? Without operable wind-shear alerts, airlines cannot guarantee safe operation of their planes, which increases the dangerousness of commercial flying.
2. Numerous clock failures occurred, including one in a federal building in Omaha, Neb. This Y2K-related glitch resulted in a security system door remaining open. Other incidents included difficulty with clock synchronization in the energy management system computers of several electrical utilities. (Source: *The Los Angeles Times*, January 2, 2000.) What would have happened if the clocks in federal buildings and utility companies around the globe had suddenly stopped, allowing open access to normally secure federal buildings? What if everyone had lost electricity for an indeterminable amount of time?
3. Amtrak's control center lost the ability to retain train symbols and thereby automatically track trains. (Source: *The Los Angeles Times*, January 2, 2000.) What if technicians had not devised a contingency plan that enabled them to enter the train numbers manually? There could have been numerous train collisions throughout the United States.

The global Y2K remediation experience has helped us all understand the impact of technology on our businesses and our lives. It has drawn the world's attention to our increased reliance on computers, technology and the professionals who manage IT. International Data Corporation's Project Magellan, a twelve month real-time research project assessing Y2K readiness around the globe, estimates remediation costs totaled as much as $320 billion worldwide, of which $134 billion was spent by the United States.

The Y2K issue gave the world no choice but to modernize its computer systems, but it was surprising how well the world, particularly industrialized nations, stepped up to the challenge, making it through the date change unscathed in the area of critical infrastructure. This should be a resounding clarion call to our government and big

business that other nations who predominantly use U.S.-manufactured technology are running neck and neck with the United States. As we enter the first decade of the new millennium, the digital playing field appears to be leveling off. We all believe the new economy of the 21st Century is going to be electronic, and we can now be sure that countries around the world are positioned to be stronger global competitors.

Last year, on a business trip to Bangalore, India, I saw thousands of Indian IT workers doing Y2K code conversion for U.S. companies. These same workers, with buckets of experience, will now be building IT products and services for a global marketplace.

In the technology industry, it is widely accepted that e-commerce is the next big-business wave to catch. Bandwidth is the only thing holding back increased business and consumer spending on the World Wide Web. According to a recent *CIO* Internet Attitudes Study, the majority (76%) of business/IT executives reported that e-commerce is currently an extension of their companies' overall business model, with 24% indicating it is a core part of the model. This trend is projected to shift by the Spring of 2001 when 39% of surveyed executives predict e-commerce will be an extension of their business model and 58% predict it will be part of the core. As bandwidth increases around the world this competition will intensify.

Now that we are on the other side of Y2K and massive remediation, we are seeing some unexpected benefits as a result of remediation. Businesses and the federal government are now painfully familiar with the technology resources and systems they run and their importance in maintaining daily business operations. Antiquated computer systems have been thrown out, modernized, patched or replaced. The public and private sector have worked together on a major world problem, successfully tackled the problem and subsequently opened channels of communication that could be the means to new economy partnerships. The future of business is one where the boundaries between companies are becoming increasingly blurred—competitors are collaborating, many members of supply chains have linked into a common technology-enabled system or process and companies are going "virtual" by outsourcing and contracting many parts of their businesses. Y2K should make people more confident in our nation's ability to thrive in such a world.

The Y2K revolution has afforded the federal government the opportunity to modernize its computer infrastructure. Now is the time for the United States to leverage its experience and utilize these newly revitalized systems to better enable the business of governing. For example, this experience base and infrastructure could enable electronic voting, registering to vote and eventually voting online; it could enable the modernization of the Internal Revenue Service and U.S. Customs, and it could create wired communities where police, fire departments and schools are all linked to their townspeople.

The most recent American century of economic reign may be followed by a second 100-year reign. However, in order to accomplish this, we must institute an agenda of enlightened legislation on Internet taxation, how America will govern using technology,

closing the digital divide between the "haves" and the "have-nots," encryption export, privacy and intellectual property rights. Our national not-too-long-term strategy must be for the U.S. to wean itself of its dependence on foreign IT workers; to that end we must craft new legislation on H1B visas. In addition, we should consider enlightened technology education legislation with the goal of providing equal technology access to all students in K-12 schools. Our goal should be to find the next Bill Gates, Steve Jobs and Steve Case, and at an early age. Doing so will ensure America's continued dominance in IT for decades to come.

The world's IT workers did a commendable and historic job on Y2K. In fact, they did such a great job, I'd like to see this House subcommittee take the lead and send a letter of recommendation to the Nobel Prize awards committee calling for a special Nobel Prize in October recognizing the collaboration of government and the private sector to minimize Y2K complications.

Technology is here to stay. On the horizon, we will be facing related and evolving issues like infrastructure protection, the privacy of "e-consumers," vulnerabilities to increased dependencies, e-commerce and the great digital divide. Will the United States continue to be a pioneer, or will we be left behind by the other countries that are suddenly on our heels?

Thank you for the opportunity to share my testimony.

Mrs. MORELLA. I think that is a fitting way to end the testimony of the panelists with this concept of the Nobel Prize and the fact that it is a great example, as you said, a feat greater than or as great as the pyramids. Ms. Hotka had some very glowing things to say about what we learned also. Coming from the private sector, it is particularly important.

We have a roll call vote right now, a quorum, but we will be back for some questioning, so I would imagine 10 minutes or so. So we will recess this hearing for about 10 minutes.

[Recess.]

Mrs. MORELLA. I am going to reconvene this hearing. I can ask a few questions, and then if other Members come in in the meantime, they can continue to ask questions.

Of course, our policy has been that if it is acceptable to you, that we might also submit questions to you by Members who may not be here. Thank you. I appreciate that.

You know, I think there have been many, many benefits to the Y2K work that has been done, whether or not it is the dimension of the pyramids or Nobel Peace Prize, but certainly there has been a lot of cooperation that has been so comprehendible. In going to the command station on December 31st, I saw many people from the private sector on their own time, unpaid, who were there for 24 hours and spent their New Years' Eve there, and then part of New Years' morning there also.

I also saw a report that National Institutes of Standards and Technology did a lot of work with small businesses in remediation of the Y2K computer bug, and the small businesses have said they thought this was a concept that they hoped would continue, the idea of being able to get help and get assistance from somebody, an agency or whatever, that cared about them.

So, again, it is another example of the private sector benefiting from what the public sector had done.

Then just the other day at the District of Columbia hearing, both Chairman Horn and I are on that authorizing committee, I asked Mayor Williams about it, because, as you may remember, the District of Columbia was so far behind, and he was very excited about the results, the fact that they have now been able to update their computer system, they know what they have, and because technology will play such a big role, particularly as we try to revitalize the District of Columbia, that they feel they are going to benefit greatly by it. Also by working with neighboring communities too.

So, again, the whole concept you all pointed out, and that is, building on the various linkages and the partnerships.

Well, I am going to ask you a question that deals with people. The vast Y2K repair corps is now being scattered to the winds after apparently saving the world from the Y2K disaster. So now what are these people trained to correct Y2K, probably those people who knew could balance, what do they do now? Can these displaced Y2K workers help to alleviate the H1B situation? What do you see with regard to the whole personnel issue? I will start with any one of you.

Ms. Hotka, why don't we start with you first.

Ms. HOTKA. Just briefly, one of the things that struck us about the people that worked on this was their ability to deal with busi-

ness units. IT does not live in a vacuum, and this was never an IT problem.

These people went out and spent time in warehouse facilities with people who run the trucks, with suppliers, with the accounting offices and all through the business. What we are seeing in our industry is that those people will continue to work in these companies and that they will continue to work with these business units to make sure that the IT tools that are created are actually used and are used effectively. That is a skill. These are generally older people, people over 30, and they have got——

Mr. MILLER. Speak for yourself.

Ms. HOTKA. Well, I am saying that because there is a tremendous emphasis, I think, in some parts of the IT world on people who are very young, who have experience in new technologies. But some of us who are not that young have some experience that might be useful, and we are finding that it is being priced in these retail companies. They don't want to lose these people.

Mr. MILLER. I think, Madam Chairman, what Mr. Burbano discussed is, in the Federal Government, very similarly true in the private sector. If you take the first group of people, namely, people who are interimly the staff of an organization, in most cases when the Y2K issue became a priority for the organization internally, and the organization decided to use internal resources, they simply took other projects, put them off to the side and took those people and focused on Y2K; and now that they have gotten through most of the Y2K era, leaving aside having to get through the next 2 months to February 29th, those projects, which have been temporarily frozen, are now going to come back as high priorities, and those people are going to go back and do those projects. That is one group to think about.

The second group of people are the contractors who came in from outside to do work for customers, whether those customers were in government or the private sector. A lot of those companies, which provided those outside services, were in a situation where they anticipated very well the end of the Y2K, they knew when their projects were going to end, and so they had to do two things: No. 1, they had to find new clients so they can continue to stay in business and continue to grow their businesses; and No. 2, they had to take into account the need to upgrade the skills of their employees to do more current projects, most of which are going to be e-commerce related or somehow on the Internet revolution as opposed to the mainframe projects.

If you look at the major companies that do business and look at the revenue in 1999 versus 1998, you will see their revenue continue to go up even as the Y2K work began to drop off. The reason is that because they were able to find new customers and they were able to retrain the work force.

So not only do I think this is not going to solve the H1B problem, if you use the logic that I use in my testimony that this is going to be a Y2K renaissance, and a lot of projects were temporarily frozen while companies were getting through the Y2K problem, I think there is going to be even a bigger explosion and even more demand for IT workers. The trick is going to be, as you suggested in your question and as Ms. Hotka commented in her comments,

making sure the workers do have the retraining. The computer language skills they have are not the ones most current or most in demand, and that has to be factored into the process.

Mrs. MORELLA. I do think many of them are older, but, on the other hand, I know the University of Maryland had a special course geared toward remediation of Y2K. Mr. Beach.

Mr. BEACH. Madam Chairman, I just would like to once again mention the aspect of what human beings like most is recognition, I am dead serious in challenging you and Chairman Horn to nominate these workers for noble awards.

The international Y2K cooperation center that we heard about today, and you are familiar with, and that Bruce McConnell did an incredibly good job running, had a subset called YES Corps, which was the Y2K Experts Service Corps. I was fortunate to be on that steering committee. This group aimed to share information with 140 countries about Y2K, and currently it is migrating to another role. We all felt this network was created for tactically addressing Y2K, the network was more valuable than the actual focus on Y2K. So there is movement afoot to expound this effort.

I would like to say there is a vested interest in large businesses in whatever they can do here in the States to help small businesses, because we are all living in this giant economic supply chain. Many large businesses are even more dependent now on smaller businesses.

The H1B visa issue, I know there is a call now to bring the limit up to 200,000. Long-term what we have to do, and I addressed it briefly in my testimony, is more rather than fewer students in America are entering computer science courses, whether in California, Maryland or Massachusetts.

I chaired last summer for the Commonwealth of Massachusetts a review of the entire higher education program, and the most damning finding we found was that we were talking about older people here, but the faculty, the faculty, No. 1, is older, is not skilled in the new technologies of JAVA, XML, you name it. There is a bottleneck there. If that bottleneck is not relieved or addressed, then our country is going to continue to have to rely on H1B visa issues.

Mr. MILLER. Could I make one more point on personnel to follow on the earlier discussion of information security? That is an enormous problem, because we do not have information security specialists trained. That is one area where you can't do H1Bs, you can't send the work offshore to Ireland or Israel or India. That work has to be done with U.S. citizens.

I know President Clinton mentioned this in his national plan, and Attorney General Reno talked about it. So this is one area where the government, working with academia and business, is going to have to focus. You are going to have to convince people to go beyond their traditional education, to get additional education, plus get security clearances, because obviously, the type of people that a Federal agency or a State government wants to hire for security information, security purposes is going to need a clearance. Even you are going to find in the private sector many private-sector financial institutions and others want to get people with very

high security clearances because they are being put in very sensitive security positions.

Mrs. MORELLA. As a matter of fact, the Science Committee passed, in the first session, actually the last Congress, a computer security bill which does have the dimension of fellowships for computer security. Even that is not enough. Much more needs to be done. We have also been pushing teacher training in technology, not so much looking at the higher education, but more education from K through 12, to make sure that even those teachers know something about how to use technology because the youngsters do, so they can also inspire them.

My legislation for women and minorities and disabled in science, engineering and technology, the commission is meeting, it will be coming up with its recommendations to get more of those groups that have traditionally not been involved, involved in those fields.

Well, I thank you. I am going to now——

Mr. HORN. If you might yield on that point——

Mrs. MORELLA. I am going to recognize you for your questioning.

Mr. HORN. Your associations could do a lot of good in bringing together the people from the Silicon Valleys of this Nation, and the community college teachers in particular.

When you think that these programmers get about $60,000 when they are out of college or out of the community college, and what we need, speaking now as a Californian where we started the community college movement and we have about 107 campuses from San Diego to the Oregon border, and they should be talking to the Silicon Valley types and vice versa. Because the State will never have enough money to get the equipment that is needed to educate people on to meet the people's needs as they go into the industry. It just seems to me there ought to be a summit meeting that perhaps your group, Mr. Miller, or your group and friends in the publishing world, and getting all these people in the room.

When you think of what Jamie Escalante, the great teacher in L.A., that took young people that everybody had given up on and they got right at the top of the college boards, and it can be done. We need to do that and we need to get the Mexican Americans, Hispanic Americans, African Americans, Americans, whatever they are, into seeing a point in their lives where they can make a substantial income. That is only going to happen if we start, as the chairman here said, concerning the K through 12. That is fine. But I think the K through 13 and 14 have to be considered, where their role, really, is to be either an academic program or a vocational program. In this case it is both. You need the academic background. You also need the vocational background. And you need the opportunity to work on equipment that makes sense.

I know from what I had to go through with a very—probably the largest school of engineering west of Texas A&M, and we were just swamped with problems on equipment in the 1970's and the 1980's. Finally, our trustees stepped up to the plate and said OK, so we will pay engineers more, we will pay people in the business school more. Well, that doesn't solve all the problems, because the equipment is the problem, and the millions that takes. And that is where it is everybody's self interest to do something along that line.

Now, I don't know if you want to add anything to that or if you are willing to do that conference, but we ought to get them in the same room with the American Electronics Association and so forth.

Mr. MILLER. We tried to do that the last couple of years, Mr. Chairman. We are making progress. I think that the IT community discovered the community college system very recently in a sense. They didn't previously think of it as a resource, except for some chip manufacturing companies, which didn't see the need for a 4-year degree. So you had a couple of instances in Arizona, particularly where Maracopa Community College was training people to work in the cleaning rooms for some of the major chip manufacturers. But I think the IT industry at large didn't see the community college as a good resource.

We held our first national work force convocation at the University of California at Berkeley in January 1998, and I think that is the first time that the IT industry began to understand that the community colleges were willing to be flexible, and, frankly, they can change a lot more quickly than formal 4-year universities, I am sure you know as a former university president.

Mr. HORN. You are absolutely correct. You won't get your supply from Berkeley. They are wonderful people. It is true. They have research designs. Ph.Ds, there is a use for some of those, face it, but you want the worker people, which does take skill, which does take imagination, and some day they might be running their own Silicon Valley firm. That is the way the whole evolution of that Santa Clara Valley has happened.

Mrs. MORELLA. I used to teach, at a community college in Montgomery County.

Mr. HORN. Absolutely.

Mr. MILLER. It is happening. Yesterday the National Commission on the 21st Century Workforce had its second field hearing, it was actually held at De Anza in Silicon Valley, and I know that that is a focus of attention.

I spoke at a major event that the Houston Partnership held 3 months ago, and virtually every attendee was there from a community college. So I think the communication is starting. We are having our third convocation in Chicago in April of this year, and have invited many of the colleges to participate. The key to the community college is obviously getting support of the State legislatures to get the funding to be able to offer the courses. In most cases State legislatures do seem willing to do that.

Mr. HORN. They see it helps their economy.

Mr. MILLER. It is an economic development issue, not an education issue. That is what employers want to know, if I move my business there, where am I going to get my IT workers.

Mr. HORN. You might have covered this while I was going over to vote, but when you look at the issues that confronted the Nation that I mentioned to Mr. Koskinen on the domestic side, do you have any particular issues that relate to technology that you think we ought to have that kind of operation that we have had in the last few years where you have somebody on behalf of the President pulling these things together, if it affects the economy and efficiency of the executive branch, which is the jurisdiction of my par-

ticular subcommittee? So what would your themes be that somebody ought to be looking at?

Mr. MILLER. Well, I have a couple. One we discussed, I think, at a previous hearing, which is an information security czar. I think that the Koskinen model is also applicable to the information security area.

Right now, Mr. Chairman, if someone from academia came up and put a chart up on the wall of how information security is handled inside the government, I don't think that wall is big enough to put all the boxes up there, because it is split over so many places. Everyone is well intentioned and has good purposes.

Mr. HORN. With the Chief Information Officer role being pretty much throughout the 24 major agencies, hasn't that helped?

Mr. MILLER. That is very helpful. But, again, even there, that is just within the particular agency. We are also talking about interrelationship with the private sector, and depending on who you ask, 85 to 90 percent of critical infrastructure we have to protect is in the private sector. Yet we have to coordinate with the government. Who do we coordinate with? Do we coordinate with Mrs. Morella's favorite office, the CIAO office, or do we coordinate the NIPC, or do we coordinate with the National Security Council or the Commerce Department? It goes on and on and on.

So we are looking for simplicity. The great thing about Mr. Koskinen's office was it was a little bitty office. He couldn't do a lot. What he could do was he could be an enabler, he could be a man who cracks the whip and try to get you to move quickly. But at the end of the day, you had to do it. He was never going to try to superimpose his own bureaucracy, either on the private sector or on a government agency. That is what I mean by a czar, not somebody that literally dictates what the private sector or the Federal agencies do. Mr. Burbano has to decide what the State Department does, Mr. Cosgrave has to understand what the IRS does. But someone who can coordinate and pull that all together, I think that would be very helpful.

Mr. HORN. Well, they have a council, and I don't know how active that was before this assignment was given them, but they certainly ought to be working on the consensual part. Of course, what I am after is, and I will be putting it in shortly, is the office of management idea where the President has somebody there that knows something about management, not just the budget. Every President puts in a director that is either an accountant or politician or economist, but they don't put anybody in that knows a thing about management, that has the President's ear.

So I want to split that off, and, fine, keep the director of the budget, but make a director of management. Roosevelt had that, Truman had it, Eisenhower had it. It went downhill starting with Kennedy and right through Reagan. They all politicized the Bureau of the Budget, which were professionals, and they served every President, whether they were Democrats or Republicans. It didn't matter. It didn't matter what their party was. They were professionals. And we have lost that contingent, until we got into this situation. When we wrote the President and said look, you have got to put somebody in charge, because it is going nowhere, and nothing but procrastination, and he did. He made a good choice.

The same thing I wrote him with Rossotti. I said look, every President has put in tax attorneys and tax accountants, how about getting a chief executive for the job. And he did a great job in getting Mr. Rossotti. So you had two splendid appointments that turned agencies around.

Mr. MILLER. Absolutely. Mr. Cosgrave, who was the CIO of IRS, was previously a CEO of a company, was actually on my board of directors, and Mr. Rossotti recruited him to come and fix the Y2K problem and run that. I certainly agree with you, Mr. Chairman.

I guess another thing I would say in terms of a theme is with all due respect to my friends in the Federal Government who bemoan the fact there are not enough Federal IT workers, I think they are trying to stop this tide, and they are not going to win this battle. We try to help them, we meet with CIO council, et cetera, to try to figure out how the Federal Government is going to recruit more IT workers. But I think in the long-term trend they are going to lose.

If they are going to lose, I would rather see them focus attention on the transition to a world where there is much more IT functionality outsourced, rather than trying to constantly refight this battle of what are they going to rejigger in the OPM manual to somehow recruit a few more IT workers. And that does not slight the Federal IT work force. I think they are great people. But I think they are just fighting a losing trend, because the delta between the Federal sector pay and the private sector pay is getting bigger and bigger. The benefits for people going into the private sector are much higher.

My members never liked to voluntarily attract someone out of the Federal marketplace, because they are making their customers mad at them, but the reality is you can't throw away a resume when someone sticks one in your hand and says I want to get paid 25 or 30 or 50 percent more, I want to come work for your company, than I can make working in the Federal marketplace.

So I think one of the issues your subcommittee wants to look at is how do you do that transition. I think it is going to happen, and to do it smartly rather than constantly trying to smart stop the tide I think would be a much more productive use of resources.

Mr. HORN. We would welcome any thoughts you have on this. I know we are already in touch with you at the staff level for the computer security hearing coming up soon.

Mr. BEACH. Mr. Chairman, I would like to comment briefly on your summit idea. I think that it is a very good idea and encourage you to consider submitting an op-ed piece we could run in CIO Magazine that would bring it to the attention of about 300,000 people.

I like the idea of director of management for one reason. Again, I was referencing earlier the CIO Know Pulse Poll that we recently did that shows within 18 months, 6 in 10 in the private side of the business are going to have e-business, and it is going to be their core business model. And how you have kept the feet to the fire for the Federal agencies here leading up to Y2K, I think this director of management, whoever he or she is, should have as one of their tasks to make certain that all the agencies and the millions and billions of dollars that the U.S. Government has spent to upgrade

its systems, how are these being used, what new services, what new applications are you providing for getting our bang for a buck.

Getting back to the previous question, Mr. Rossotti mentioned I think that in the IRS, they upgrade each year one-third of their computers. So what happens to the third that are being thrown out? Where are these going? The other issue is there is a great opportunity in the junior colleges and the 4-year schools for the faculty could be adjunct faculty from the business community. These are the men and women who know most about its leading technologies. I would encourage a program of adjunct faculty to our Nation's community colleges are 4-year schools.

Mr. HORN. You are absolutely correct, because the research universities are simply too involved in long-term research, which does have a payoff in many ways. A lot of our industry is based on that research. But in terms of getting a curriculum turned around, as you correctly viewed, that can happen much more easily in a community college. Rather than have the faculty say let's think about this for 3 years.

So that is part of the problem. This is a national crisis in skills. On the Clinger-Cohen Act, we are focusing partly on the information technology human resources issues and the need for qualified individuals and managers when that comes up.

And that's another one coming up in the next few weeks. So let me skip to something else that isn't as serious as what we've had here, but I guess I'd want to ask Ms. Hotka that I'm just curious with the wonderful technology we have to trace everything in the stores of America, do you know how many generators were turned in?

Ms. HOTKA. We were sure, Mr. Chairman, that we would see this mass return of generators which would then be refused at the store level by stores who said that they wanted to sell it to you instead of lend it to you. We were amazed instead that stores used this as a customer retention mechanism. They said please, come back and return it and while you're here, buy something else.

Mr. HORN. I was educated yesterday by my staff when I raised this that there was such a thing as a stocking fee and tell me about that.

Ms. HOTKA. What some of our retailers did was to charge a restocking fee so that if you brought back the generator after January 1 in the box because you didn't need it, that they would charge 20 percent. Some of them did that, did in fact charge that fee but some of them I think surprised all of us and used this as a way to get those valued customers back into the store and while they were there, by the way, why don't you buy this Christmas tree which is on deep discount and it worked beautifully. We saw very little demand—that was one of the things that surprised us too. We thought that the public was going to flock into stores at the end of the year and buy all kinds of stuff. We didn't see it at all.

Mr. MILLER. If I could make one point about your CIO elevation on the last question, I want to bring to your attention a new institution which the Virginia secretary of technology Don Upson is creating called the CIO Academy. I don't know if he's publicly rolled this out yet, but I know he's already recruited several State CIOs to be on the board of directors.

He's recruited Jim Flyzik who is the CIO of the Department of Treasury who was kind enough to ask me to do it. He's got some other people from the private sector. I think this relates to the whole issue that you, of course, implemented within Clinger Cohen which is elevating the whole position of the CIO within the organization.

And obviously one of the major roles that Mr. Beach's publication does is it also creates a network through his publication, his polls, his meetings he sponsors. I think Secretary Upson tends to do this in a much more educational level. I think you're going to see more and more where this is going.

Now, the challenge, and I think, Mr. Beach, you had an article in your publication recently about whether the CIO job will even exist in 5 years. You had some futurists discussing that. I think one of the conclusions was there would be no such position, maybe a chief knowledge officer or something else like that but there wouldn't be a CIO because technology will become so ubiquitous that the idea that you have a specialist would be like saying you have a telephone specialist. That won't exist anymore.

Generally, I think business and government are paying a lot more attention to the whole role of the CIO and part of it is because of Y2K again. It all rolls back to the fact that Y2K suddenly brought to the attention of the CIO and the CFO and board of directors that this guy or gal who ran the technology wasn't some person who you could just put off on the side of the back room, that he or she was fundamental to your strategic business or strategic government delivery of services.

Mr. HORN. In educating a CIO, what is your percentage of technology versus management skills?

Mr. MILLER. I'd say knowledge of technology is somewhere between 5 and 10 percent, management understanding business, understanding the core operation is probably about 90 percent. I think the same way as a CFO. I don't think you expect the CFO to be your bookkeeper. The CFO is your financial planner, business organizer. I think the same thing is true of your CIO you don't expect him or her to be necessarily the chief technical person, that he or she is the person who is looking at how the technology fits into the business organization. Mr. Beach probably has some surveys on that I'm sure.

Mr. BEACH. We've got lots of them. It's along with what Harris said. I mentioned it several times here today that what has happened is that technology and e-business and e-commerce and the overuse of the letter "E" but what has happened is that there has got to be an extension to a company's business model. So technology has gone from being an extension of how we govern to being the core—a core part of that infrastructure of how we govern.

I would agree with the percentages of Harris that the more successful CIOs that I see are those men and women who have a keen understanding not of technology but of their customers because then they could always use technology to service that customer need rather than saying I know everything about fiber and all this other stuff, you say let's go find a customer to satisfy that. So they are more customer-focused, and smart businesses and smart gov-

ernments are realizing that technology is going to be a core platform in terms of how they provide a good or service.

Mr. HORN. Does your magazine take a look at how Y2K made us learn that we can now better manage the operation once we had to get in and say let's merge this system with that system or let's just get rid of it? To what degree do you see that movement in the executive branch?

Mr. BEACH. In the executive branch here in Washington?

Mr. HORN. Right or the field.

Mr. BEACH. I think the lesson learned from the CIOs in the private sector, what Y2K taught them is that no one is an island, that all these businesses are connected in these global supply chains. And I can't comment particularly on the question of executive branch, but I would say that you—no one aspect of the government, whether it's legislative, the judicial, or the executive is—it's never been that way, but technology is giving each of those branches a better opportunity to communicate and share information and govern in ways that we haven't thought of.

Ms. HOTKA. If I can expand on that too. I think one of the things that we found was Y2K was such a flash point, that if I called up someone from a company who's not a member and said I need to talk to you about Y2K, I could get that person on the phone instantly. It cut across all kinds of company barriers.

There was no competitiveness at all. We had an immovable deadline and an issue that everybody understood and so everyone was willing to talk to everyone. If we can come to some kind of goal like that, obviously we'll not have this again. And thank God for it, but if we could come up with some kind of goal for technology literacy and for good corporate use of IT, we could again get to that point where I could pick up the phone and get anybody on the phone and be able to cooperate. It was useful. If we can harness that again it would be terrific.

Mr. HORN. I think you're right. I've got just one or two things to say here, and then I'm going to leave and Mrs. Morella, she reminds me we have a conference, all of us at 1 p.m. Let me say without objection, I want to file within the testimony when after Mr. Koskinen, an exchange of letters between the Secretary General of the United Nations and myself.

Mrs. MORELLA. Without objection, so ordered.

Mr. HORN. No. 2, I would like to thank the following people that have been involved and not just in this hearing but in most of our hearings. From the subcommittee on Government Management, Information, and Technology, J. Russell George, staff director and chief counsel; Matthew Ryan, senior policy director; Bonnie Heald, director of communications and professional staff member; Chip Ahlswede, chief clerk and unfortunately it's his last hearing with us; Deborah Oppenheim, intern; and minority staff, Trey Henderson, the counsel; and Jean Gosa, minority staff assistant; and for the Technology Subcommittee of the House Committee on Science, Jeff Grove, staff director; Ben Wu, counsel; Vicki Stackwick, staff assistant; the technical minority staff is Michael Quear, the professional staff member; and Marty Ralston, staff assistant; and our two court reporters today are Bob Cochran and Laurie Harris. And we thank you all for what you're doing.

In closing on my behalf, I would say governments and industries worldwide have benefited from this experience. I think that testimony was very clear today. This problem has many silver linings as our witnesses have described. There are equally as many if not more people who have worked tirelessly in an effort to solve the year 2000 computer problem, and we saw some of them before us today. Obviously Mr. Koskinen is Assistant to the President and Chair of the Council on the Year 2000 Conversion. The General Accounting Office staff, particularly that staff headed by Mr. Willemssen, who was here today. Federal, State, and local government personnel, the private sector, individual grass roots organizations, and the two staffs I've mentioned and the technology subcommittee which has been our partner in overseeing this massive and unique experience and we thank them and this success demonstrates what can be accomplished with leadership, focus, and dedication, and it's a great legacy to begin this new millennium and we thank all of you for your hard work. I thank the chairwoman.

Mrs. MORELLA. I thank you, Mr. Horn. You've expressed it very well for all of us. Hardly a time to ask another question. I guess my final one is now as we look into the near future, any comments about February 29 and this concept of windowing? Has that been taking place and is it anything that we should be looking into, comment on, enlighten the public on? Mr. Miller.

Mr. MILLER. The companies would take the same attitude that you heard expressed by Mr. Koskinen and the panel this morning. They don't expect very many problems with February 29, but they are maintaining diligent oversight of the problem. Every leap year there's a problem.

I hate to tell you, whether it's supposed to be or not supposed to, there's problems so it's not unique. I think there will be diligence, but I wouldn't expect any major problems. As far as windowing again, in a way it's postponing the problem. I think the expectation is it's been postponed long enough. It will be OK, but we got fooled last time around. There's another windowing problem which you may know about, which is not necessarily this subcommittee's concern, which there is a gentleman who has a patent on windowing who wants a lot of companies to pay him a lot of money for that. But that right now is a matter before the patent office and perhaps a matter before the court so probably Congress doesn't want to touch that one right now.

Ms. HOTKA. When we did our testing, when retail companies went through and tested all the systems they thought were fine, the No. 1 thing that came up with was leap year. We don't expect the world to come to an end. We think you'll still be able to shop, but if I had to pick one thing that I thought was going to be funky that is it. We'll be in the ICC again.

Mr. BEACH. I would just make a comment on the windowing that I believe Eduardo and the previous panel mentioned it that keeping an inventory of those applications that have been windowed might be wise. I'd like to know where those are in 20 years. I don't think we should make the mistake that we made in the 1960's and 1970's that these applications are not going to——

Mrs. MORELLA. Exactly. Even when you think of the 1980's, the 20-year span whoever thought we would now be in the year 2000. Any final comments that you'd like to make? I want to thank you all very much for again being here, sharing your expertise, and also for all that you have done to make this Y2K millennium bug be squashed. I thank you very much. So we now adjourn the meeting.

[Whereupon, at 1:07 p.m., the subcommittee was adjourned.]

[The prepared statement of Hon. James A. Barcia follows:]

Statement

Hon. James A. Barcia

Subcommittee on Technology

The Year 2000 Computer Problem:
Did the World Overreact and What Did We Learn?

27 January 2000

I would like to join my colleagues in welcoming everyone to this morning's hearing. I appreciate the efforts of our witnesses to finish their testimony even though the Federal government was closed for the past two days as a result of this week's snowstorm. Of course, those of us from Michigan think of this as just a normal part of winter.

Today's hearing is the last in a long series on the Y2K computer problem. First, I want to commend our federal agencies for their hard work on successfully addressing this problem. Agencies received quite a bit of criticism for their efforts and many concerns remained until the very last moments before the rollover. However, the final evidence proved that agencies had successfully addressed the problem. There were no disruptions of federal agencies' public services. Indeed, the Y2K turnover actually caused less disruption than this week's snowstorm.
In retrospect, as this hearing's title highlights -- did we overreact and spend too much? There were no disruptions of power grids, the air traffic control system worked flawlessly, small business operations continued without interruption and there has not been an avalanche of Y2K-related litigation. Of course, in hindsight it's easy to ask these types of questions. But, we need to carefully review our actions and learn from the experience. I really have only a few basic questions:

In the final tally, how much did the Federal government spend on it's Y2K remediation efforts?

What did we learn? Were the assessments of the extent of the problem and the actions taken accurate and appropriate?

Finally, why were predictions of the Y2K disruptions in some foreign countries overestimated, for example, we evacuated most personnel at our Embassy in Moscow over fears of widespread Y2K disruptions?

Again, I would like to thank each our witnesses for appearing this morning. I look forward to hearing their testimony.

○